PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-161162
(43)Date of publication of application : 18.06.1999

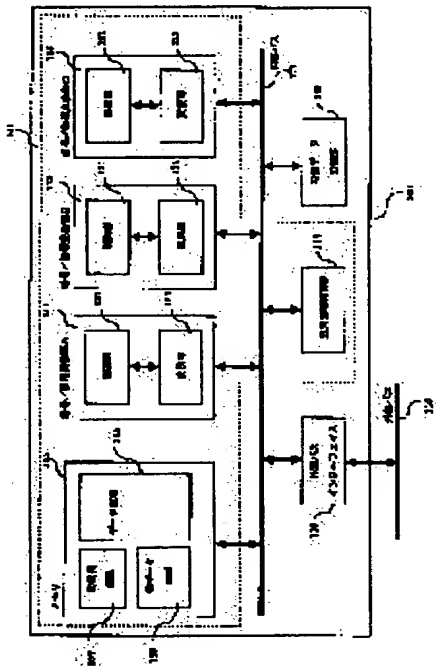
(51)Int.Cl. G09C 1/00
G09C 5/00
H04L 9/06

(21)Application number : 09-326455
(22)Date of filing : 27.11.1997

(71)Applicant : HITACHI LTD
(72)Inventor : AIKAWA SHIN
TAKARAGI KAZUO
FURUYA SOICHI
HIRAHATA SHIGERU

(54) CIPHERING METHOD OR DECIPHERING METHOD, AND DEVICE USING THE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To increase the processing speed of conversion in CBC mode by simultaneously encoding conversion and decoding conversion for blocks taken out of frames wherein a message is divided, one by one.
SOLUTION: In a data area 135, data as objects of ciphering or deciphering conversion are written in order from outside a ciphering/deciphering conversion system 101 and then divided into frames. The frames are each a bit sequence which is longer than the block length as the basis conversion unit of block ciphering conversion. The data written in the data area 135 are read in ciphering/deciphering conversion parts A111 to C113 in parallel and ciphered or deciphered, and the results are written in the data area again. Consequently, the data in the data area 135 are ciphered or deciphered. The data in the data area 135 after the ciphering or deciphering conversion are read sequentially out of the ciphering/deciphering conversion system 101.



LEGAL STATUS

[Date of request for examination] 19.01.2001
[Date of sending the examiner's decision of rejection] 13.07.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－161162

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.[6]		識別記号	Ｆ Ｉ		
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ａ
	5/00			5/00	
Ｈ０４Ｌ	9/06		Ｈ０４Ｌ	9/00	６１１Ｚ

審査請求　未請求　請求項の数19　ＯＬ　（全 31 頁）

(21)出願番号　特願平9－326455

(22)出願日　平成９年(1997)11月27日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　相川　慎
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マルチメディアシステム開発本部内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

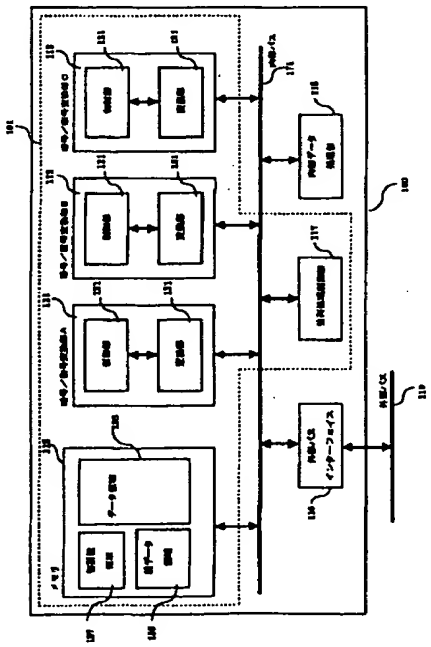
(54)【発明の名称】　暗号化方法または復号化方法およびそれを用いた装置

(57)【要約】

【課題】データの暗号変換および復号変換を並列に処理することができる、暗号／復号変換システムを提供すること。

【解決手段】暗号および復号変換を行う情報処理機器に、複数の演算を並列に行う、複数の演算手段を備え、暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、暗号変換および復号変換を行う構成にする。

図１



1

【特許請求の範囲】

【請求項１】複数の演算を並列に行う、複数の演算手段と、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割する手段と、

複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、前記複数の演算手段に、並列に入力する手段とを備えることを特徴とする並列暗号化装置。

【請求項２】複数の演算を並列に行う、複数の演算手段を用い、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、

複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、並列に、暗号変換する処理を行うことを特徴とする並列暗号化方法。

【請求項３】複数の演算を並列に行う、複数の演算手段と、

復号変換すべき暗号文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割する手段と、

複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、前記複数の演算手段に、並列に入力する手段とを備えることを特徴とする並列復号化装置。

【請求項４】複数の演算を並列に行う、複数演算手段を用い、

復号変換すべき暗号文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、

複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、復号変換する処理を行うことを特徴とする並列復号化方法。

【請求項５】複数の演算を並列に行う、複数の演算手段と、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割する手段と複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、前記複数の演算手段に、並列に入力する手段と、

復号変換すべき暗号文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割する手段と、

複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、前記複数の演算手段に、並列に入力する手段とを備えることを特徴とする並列暗号化／復号化装置。

2

【請求項６】複数の演算を並列に行う、複数演算手段を用い、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、

複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、並列に、暗号変換する処理を行い、

復号変換すべき暗号文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、

複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、並列に、復号変換する処理を行うことを特徴とする並列暗号化／復号化方法。

【請求項７】複数の演算を並列に行う、２個以上のＮ個の演算手段を含む暗号変換装置であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、一つのフレームから２乃至Ｎ個のブロックを取り出して、取り出した２乃至Ｎ個のブロックを、同時に、該暗号変換装置に入力することを特徴とする並列暗号方法および装置。

【請求項８】複数の演算を並列に行う、２個以上のＮ個の演算手段を含むコンピューターの制御方式であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、一つのフレームから２乃至Ｎ個のブロックを取り出して、取り出した２乃至Ｎ個のブロックを、同時に、暗号変換する処理を含むことを特徴とする並列暗号方法および装置。

【請求項９】複数の演算を並列に行う、２個以上のＮ個の演算手段を含む復号変換装置であって、

復号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、一つのフレームから２乃至Ｎ個のブロックを取り出して、取り出した２乃至Ｎ個のブロックを、同時に、該復号変換装置に入力することを特徴とする並列復号方法および装置。

【請求項１０】複数の演算を並列に行う、２個以上のＮ個の演算手段を含むコンピューターの制御方式であって、

復号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、一つのフレームから２乃至Ｎ個のブロックを取り出して、取り出した２乃至Ｎ個のブロックを、同時に、復号変換する処理を含むことを特徴とする並列復号方法および装置。

【請求項１１】複数の演算を並列に行う、２個以上のＮ個の演算手段を含む暗号／復号変換装置であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本

単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、一つのフレームから２乃至Ｎ個のブロックを取り出して、取り出した２乃至Ｎ個のブロックを、同時に、該暗号／復号変換装置に入力する、並列暗号方法、および、復号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、一つのフレームから２乃至Ｎ個のブロックを取り出して、取り出した２乃至Ｎ個のブロックを、同時に、該暗号／復号変換装置に入力する、並列復号方法、を用いることを特徴とする並列暗号／復号方法および装置。

【請求項１２】複数の演算を並列に行う、２個以上のＮ個の演算手段を含むコンピューターの制御方式であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、一つのフレームから２乃至Ｎ個のブロックを取り出して、取り出した２乃至Ｎ個のブロックを、同時に、暗号変換する、並列暗号方法、および、復号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、一つのフレームから２乃至Ｎ個のブロックを取り出して、取り出した２乃至Ｎ個のブロックを、同時に、復号変換する、並列復号方法、を用いる処理を含むことを特徴とする並列暗号／復号方法および装置。

【請求項１３】複数の演算を並列に行う、複数の演算手段を含む暗号変換装置であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、該暗号変換装置に入力し、複数個の暗号文ブロックを出力し、該複数個の暗号文ブロックを、再度、該暗号変換装置に入力することを特徴とする並列暗号方法および装置。

【請求項１４】複数の演算を並列に行う、複数の演算手段を含むコンピューターの制御方式であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、暗号変換し、複数個の暗号文ブロックを出力し、該複数個の暗号文ブロックを、次に暗号変換する、複数個の平文ブロックの暗号変換に用いる処理を含むことを特徴とする並列暗号方法および装置。

【請求項１５】複数の演算を並列に行う、複数の演算手段を含む暗号変換装置であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本

単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、該暗号変換装置に入力し、各複数ブロックに対して、暗号変換を行い、各暗号変換途中に得られる、複数個の中間ブロックを、再度、暗号変換装置に入力することを特徴とする並列暗号方法および装置。

【請求項１６】複数の演算を並列に行う、複数の演算手段を含むコンピューターの制御方式であって、

暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、暗号変換し、各暗号変換途中に得られる、複数個の中間ブロックを、次に暗号変換する、複数個の平文ブロックの暗号変換に用いる処理を含むことを特徴とする並列暗号方法および装置。

【請求項１７】装置Aと装置Bと装置Cは、お互いに暗号通信できるように構成されており、前記装置Aまたは前記装置Bから前記装置Cに送信されたデータは、暗号変換されないままであるかどうかを前記装置Cが検査する手段と、該データが暗号変換されないままであることが検知された場合には、そのことを示す信号を別の装置Dに送信する手段とを備えること特徴とする暗号通信システム。

【請求項１８】前記装置Dは、前記データが暗号変換されないままであることが検知されたことを示す信号を受信した場合、前記装置Dから前記装置Aまたは前記装置Bに送信するデータを制限する手段を有することを特徴とする請求項１７記載の暗号通信システム。

【請求項１９】前記装置AまたはBは装置Eと通信できるように構成されており、

前記装置Eは前記装置Aに平文データを暗号方式１により暗号化した暗号文１を送る手段を備え、

前記装置Aは該暗号文１を該暗号方式１に対応する復号方式１により復号する手段と、

もとの平文データを得た後、暗号方式１とは異なる暗号方式２で平文データを再暗号化して暗号文２を得た後、前記装置Bに暗号文２を送信する手段とを備えることを特徴とする請求項１７記載の暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータ、情報処理装置、情報家電機器等の間で伝送されるデータの、暗号／復号技術に関するものである。

【０００２】

【従来の技術】近年の、パーソナルコンピュータや、デジタル情報家電の普及に伴い、画像、音声、データなどのマルチメディア情報を機器間でやり取りする機会が増えてきた。マルチメディア・データは、デジタル・デー

タなので、簡単に複製できてしまい、不正コピーや、著作権侵害などが、大きな問題となっている。この問題を解決するには、暗号技術が必須となる。機器間を接続する通信路上を流れるデータを暗号化することで、盗聴および改ざんを防止し、不正コピーを防ぐことができる。データの暗号化に関しては、ブロック暗号を用いる場合が多い。

【０００３】ブロック暗号とは暗号化したいデータを一定長のデータ（ブロックデータ）に分割し、ブロック単位に、同一長の暗号データに暗号化する共通鍵暗合方式である。ブロック暗号においては、通常一定の期間に同一の暗号鍵が使用されるため、同一のブロックデータがいつも同一の暗号データに変換されることになり、安全上あまり望ましくない。そこで、その対処法として、ブロック暗号の利用モードのある暗号文ブロック連鎖（Cipher Block Chaining, ＣＢＣ）モードを用いることが多い。以下、ＣＢＣモードによる暗号変換および復号変換方式についての説明を図２４を用いて行う。ここで、ブロックデータの長さは64ビットとして説明していく。図２４において、2001から2003はブロック暗号変換部であり、2011から2013はブロック復号変換部である。すべてのブロック暗号部およびブロック復号部は、同じ鍵データを用いる。また、2021から2026は排他的論理和演算部である。

【０００４】まず、ＣＢＣモードによる暗号変換について説明する。暗号化したいデータ（平文データ）は、先頭から、64ビット長のブロックデータに分割されていく。これを平文ブロックと呼ぶ。図２４においては、平文データは、平文ブロックM[1]241、平文ブロックM[2]242、平文ブロックM[3]243、... というように分割されていく。平文ブロックは、暗号変換され、暗号文ブロックとなる。最初の平文ブロックM[1]241の暗号変換には、64ビット長の初期値IV2061を用いる。M[1]241と初期値IV2061は排他的論理和部2021で、排他的論理和をとった後に、ブロック暗号部2001で暗号変換されて、暗号文ブロックC[1]251になる。次に、平文ブロックM[2]242は、暗号文ブロックC[1]251と排他的論理和部2022で、排他的論理和をとった後に、ブロック暗号部2002に入力され、暗号化されて、暗号文ブロックC[2]252になる。以下、同様の処理を、繰り返して、暗号文ブロックを生成していく。変換された、暗号文ブロックを順番に結合したものが、暗号文データになる。以上が、ＣＢＣモードによる暗号変換である。ＣＢＣモードによる暗号変換は、直前に変換した暗号文ブロックを、順次、フィードバックしていくので、最初の平文ブロックから順番に変換していく必要がある。

【０００５】次に、ＣＢＣモードによる復号変換について説明する。前述したＣＢＣモードによる暗号変換で、暗号変換された、暗号文データは、暗号文ブロックC[1]251、暗号文ブロックC[2]252、平文ブロックC[3]253、... というように分割されていく。最初の暗号文ブロックC[1]251の暗号変換には、64ビット長の初期値IV2061を用いる。これは、前述の暗号変換の際に用いた初期値と同じ値である。C[1]251は、ブロック復号部2011で復号変換して、初期値IV2061と、排他的論理和部2024で、排他的論理和をとって、平文ブロックM[1]241になる。

【０００６】次に、暗号文ブロックC[2]252は、ブロック復号部2012で復号変換して、暗号文ブロックC[1]251と排他的論理和部2025で、排他的論理和をとって、平文ブロックM[2]242になる。以下、同様の処理を、繰り返して、平文ブロックを生成していく。生成された、平文ブロックを順番に結合したものが、平文データになる。以上が、ＣＢＣモードによる復号変換である。ＣＢＣモードによる復号変換は、前述したＣＢＣモードの暗号変換とは異なり、変換結果は、フィードバックされない。

【０００７】

【発明が解決しようとする課題】前述したように、ＣＢＣモードによる暗号変換は、最初のブロックデータから順番に処理していく必要があるので、高速処理の妨げとなっていた。

【０００８】本発明の目的は、ＣＢＣモードによる暗号変換および復号変換の処理速度を向上させることにある。

【０００９】より具体的には、データの暗号変換および復号変換を並列化する手段を提供し、暗号変換および復号変換の処理速度を向上させることにある。

【００１０】

【課題を解決するための手段】上述した目的を達成するため、暗号および復号変換を行う情報処理機器は、複数の演算を並列に行う、複数の演算手段を備え、暗号変換すべき平文メッセージを、ブロック暗号の基本単位である１ブロック長よりも長い、ビット列を１フレームとする、複数フレームに分割し、複数フレームから１ブロックずつデータを取り出して、取り出した複数ブロックを、同時に、暗号変換および復号変換を行う。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。

【００１２】図１は、本発明の第１実施形態に係る、暗号／復号変換システムを内蔵した、情報処理機器の構成図である。図１において、100は情報処理機器、119は外部バスである。また、情報処理機器100は、暗号／復号変換システム101と、外部バスインターフェイス116と、内部データ処理部118が、内部バス171で接続された形態で構成されている。情報処理機器100は、外部バス119を介して、他の機器から暗号文データを受け取り、暗号／復号変換システム101で、復号化して、平文データを得て、内部データ処理部118でデータ処理をする機能と、内部データ処理部118から、出力される平文データを、

暗号／復号変換システム101で、暗号化して、暗号文データを得て、外部バス119を介して、他の機器に送信する機能を持っている。このような情報処理機器100の具体例として、たとえば、デジタルＶＴＲや、デジタル放送受信機内蔵ＴＶなどが考えられる。

【００１３】暗号／復号変換システム101は、暗号／復号変換部Ａ111と、暗号／復号変換部Ｂ112と、暗号／復号変換部Ｃ113と、メモリ115と、並列処理制御部117とで構成される。

【００１４】暗号／復号変換部Ａ111と、暗号／復号変換部Ｂ112と、暗号／復号変換部Ｃ113は、制御部121と、変換部131で構成される。変換部131は、従来の技術で説明した、ＣＢＣモードによる暗号変換および復号変換を行う。

【００１５】メモリ115には、データ領域135と、鍵データ領域136と、初期値領域137に分割される。データ領域135は、暗号／復号変換するデータを一時的に保存する領域である。鍵データ領域136は、暗号／復号変換に用いる、鍵データを保存する領域である。初期値領域137は、ＣＢＣモードにおける、暗号／復号変換の際に用いる初期値を保存しておく領域である。ここで、鍵データおよび初期値は、暗号通信を行いたい機器間で、共有しておく必要がある。本発明においては、機器間での鍵共有については直接関係しないので詳細は省略することにする。

【００１６】データ領域135には、暗号／復号変換システム101外部から、暗号あるいは復号変換を行いたいデータが、順次、書き込まれてくる。データ領域135に書き込まれてくるデータは、暗号／復号変換部Ａ111と、暗号／復号変換部Ｂ112と、暗号／復号変換部Ｃ113に、並列に読み込まれていき、暗号あるいは復号変換され、その結果が再び、データ領域に書き込まれていく。これによって、データ領域135内のデータが暗号あるいは復号変換処理されていく。データ領域135内の暗号あるいは復号変換処理されたデータは、順次、暗号／復号変換システム101外部に読み出されていく。

【００１７】以下、暗号／復号変換システム101が、平文データを暗号変換する手順を図２を用いて説明していく。平文データ220は、データ領域135に書き込まれ、暗号変換を行うために、フレームに分割されていく。ここで、フレームは、ブロック暗号変換の基本変換単位であるブロック長よりも、長いビット列である。ＣＢＣモードにおける暗号変換は、フレーム毎に完結するものとする。これによって、各フレームの暗号変換は、鍵データと初期値が与えられれば、独立に行うことができる。ＣＢＣモードにおける暗号変換は、従来の技術で説明したように、ブロック単位に行われるので、データ領域135に書き込まれたフレームは、ブロックに区切られる。ここで、ブロック長は64ビットとする。

【００１８】図２においては、平文フレームＡ221は、平文ブロックM[1]241、平文ブロックM[2]242、平文ブロックM[3]243、... 平文ブロックM[n]248とn個のブロックに分割される。ここで、最後の平文ブロックM[n]248の長さが、64ビット未満の場合は、端数平文ブロックとして区別しておく。同様に、データ領域135内の他の平文フレームもブロックに区切られていく。ブロックに分割された、平文フレームＡ221は、暗号／復号変換部Ａ111において、ブロック単位に、データ領域135から読み出され、CBCモードを用いて暗号変換されて、再びデータ領域135の同じ場所に書き込まれれいく。すなわち、平文ブロックM[1]241は暗号文ブロックC[1]251に変換され、平文ブロックM[2]242は暗号文ブロックC[2]252に変換され、....というように、順次ブロック列を暗号変換していく。ここで、最後の平文ブロックが端数平文ブロックの場合は、ＣＢＣモードとは異なる方法を用いて、暗号変換する。これを端数処理と呼ぶ。詳細は後述する。暗号／復号変換部111で暗号変換された、暗号文ブロックC[1]251、暗号文ブロックC[2]252、暗号文ブロックC[3]253、... 暗号文ブロックC[n]258、は、暗号文フレームＡ231として、結合される。

【００１９】同様な処理を、平文フレームＢについては暗号／復号変換部Ｂ112が、暗号文フレームＢ232に変換し、平文フレームＣ223については暗号／復号変換部Ｃ113が、暗号文フレームＣ233に変換してく。これによって、平文フレームの暗号変換を、並列に行っていくことができる。ここで、それぞれの暗号／復号変換部は、変換の前に、鍵データ領域136から鍵データを、初期値領域137から初期値データを読み込んでおく必要がある。この並列処理の制御は、並列処理制御部117が行い、それぞれの暗号／復号変換部が、平文データのどのフレームを暗号変換すればよいかを指示していく。

【００２０】以上、平文データを複数の暗号／復号変換部で暗号変換していく方法について説明したが、同様に、暗号文データを複数の暗号／復号変換部で復号変換していく手順について、図３を用いて説明する。

【００２１】暗号文データ230は、データ領域135に書き込まれ、復号変換を行うために、フレームに分割されていく。前述の暗号変換で説明したのと同様に、それぞれのフレームは、さらに、下位構造であるブロックに区切られ、暗号／復号変換部は、順次、暗号文ブロック列を読み込んで、ＣＢＣモードを用いて、平文ブロックに復号変換して、再びデータ領域135の同じ場所に書き込んでいく。ここで、最後の暗号文ブロックの長さが、６４ビット未満の場合は、端数暗号文ブロックとして区別し、端数処理によって、復号変換を行う。詳細は後述する。復号変換された、平文ブロック列は、平文フレームとして結合される。ＣＢＣモードによる復号変換は、フレーム毎に完結するので、複数の暗号／復号変換部を用いて、暗号文フレームを、並列に、復号変換していくことが可能である。この並列処理の制御は、並列処理制御

部117が行い、それぞれの暗号／復号変換部が、暗号文データのどのフレームを復号変換すればよいかを指示していく。

【００２２】次に、図１における、変換部131の内部構造について、詳細に説明する。

【００２３】図４は、変換部131の詳細構成図であり、以下のモジュールより構成される。411と412と414は３入力マルチプレクサ、413と415は２入力マルチプレクサ、421と422はレジスタ、431は排他的論理和演算部、441はブロック暗号部である。上記モジュールの入力および出力は、すべて64ビットのパラレル入出力である。ブロック暗号部441は、従来の技術で説明したように、ブロック暗号方式による暗号変換および復号変換を行う。ブロック暗号方式は、通常、暗号変換と復号変換のアルゴリズムが、よく似ているので、容易に、暗号変換と復号変換を共有できるブロック暗号器を設計することができる（たとえば、本発明者によって提案されている（特願平09-213327）に詳しい）。

【００２４】初めに、この変換部131がＣＢＣモードによる暗号変換を行う手順について説明する。変換部131には、平文ブロック列が順次入力され、暗号文ブロックを順次出力していく。一番目の平文ブロックの変換のときだけは、マルチプレクサ414を介して、レジスタ422に初期値を設定して保持しておく。平文ブロックは、マルチプレクサ411を介して、排他的論理和演算部431に入力され、一方、レジスタ422の値は、マルチプレクサ415を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値は、マルチプレクサ412を介して、ブロック暗号部441に入力され、鍵データを用いて、暗号化される。ここで、ブロック暗号部441は暗号モードに設定する。ブロック暗号部441からの出力は、暗号文ブロックとして、出力されるとともに、次の平文ブロックへのフィードバック値として、マルチプレクサ414を介して、レジスタ422の値を更新し保持される。以上の様な変換を繰り返していくことで、平文ブロックを、暗号文ブロックに順次変換していく。ここで、最後の平文ブロックが、端数平文ブロックの場合は、以下のように端数処理を行って、端数暗号文ブロックに変換する。

【００２５】端数平文ブロックは、マルチプレクサ411を介して排他的論理和演算部431に入力され、一方で、レジスタ422の値（直前の暗号文ブロック）を、マルチプレクサ415および412を介して、ブロック暗号部441で暗号変換し（このとき暗号モードに設定する）、出力結果を、マルチプレクサ413と415を介して、排他的論理和演算部431に入力する。排他的論理和演算部431の出力値はマルチプレクサ413を介して、端数暗号文ブロックとして、出力される。

【００２６】以上の処理によって、変換部131は、平文ブロック列を、暗号文ブロック列に暗号変換していくことができる。ここで、マルチプレクサのスイッチング、レジスタの値の保存と書き換え、ブロック暗号部の暗号モードの設定は、制御部121が行う。

【００２７】次に、この変換部131がＣＢＣモードによる復号変換を行う手順について説明する。変換部131には、暗号文ブロック列が順次入力され、平文ブロックを順次出力していく。一番目の暗号文ブロックの変換のときだけは、マルチプレクサ414を介して、レジスタ422に初期値を設定して保持しておく。暗号文ブロックは、レジスタ421に保持されるとともに、マルチプレクサ412を介して、ブロック暗号部441に入力されて、復号化される。ここで、ブロック暗号部441は復号モードに設定する。ブロック暗号器441の出力値はマルチプレクサ411を介し、排他的論理和演算部431に入力され、一方で、レジスタ422の値は、マルチプレクサ415を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値はマルチプレクサ413を介して、平文ブロックとして、出力される。この時、レジスタ421に保持されていた値を、マルチプレクサ414を介して、レジスタ422に保持する。以上の様な変換を繰り返していくことで、文ブロックを、暗号文ブロックに順次変換していく。ここで、最後の暗号文ブロックが、端数暗号文ブロックの場合は、以下のように端数処理を行って、端数平文ブロックに変換する。

【００２８】端数暗号文ブロックは、マルチプレクサ411を介して排他的論理和演算部431に入力され、一方で、レジスタ422の値を、マルチプレクサ412を介して、ブロック暗号部441で暗号変換し（このとき暗号モードに設定する）、出力結果を、マルチプレクサ413と415を介して、排他的論理和演算部431に入力する。排他的論理和演算部431の出力はマルチプレクサ413を介して、端数平文ブロックとして、出力される。

【００２９】以上の処理によって、変換部131は、暗号文ブロック列を、平文ブロック列に復号変換していくことができる。ここで、マルチプレクサのスイッチング、レジスタの値の保存と書き換え、ブロック暗号部441の暗号および復号モードの設定は、制御部121が行う。

【００３０】以上より、変換部131は、暗号変換および復号変換の両方を行うことが可能である。

【００３１】前述したように、暗号／復号変換システム101は、複数の暗号／復号変換部を用いて、ＣＢＣモードによるの暗号変換、あるいは復号変換を、並列に行うことができ、一つの暗号／復号変換部のみを用いた場合よりも、より高速に暗号／復号変換を行うことができる。　この暗号／復号変換システム101は、複数の暗号文データおよび平文データを、同時に、暗号／復号変換することも可能である。たとえば、図５において、暗号／復号変換システム101は、内部データ処理部118から出力される平文データＡ511を、暗号変換すると同時に、外部バスインターフェイス116が、外部バス119から受信

する暗号文データＢ521を、復号変換している。ここで、平文データＡおよび暗号文データＢは、リアルタイム・データであるとし、平文データＡの方が、暗号文データＢより、ビットレートが大きいものとする。また、暗号／復号変換部Ａ111と、暗号／復号変換部Ｂ112と、暗号／復号変換部Ｃ113の暗号変換および復号変換の処理速度は、すべて同じであるとし、単独では、暗号文データＢは、リアルタイムで復号変換できるが、平文データＡの暗号変換は、不可能であるとする。しかし、２つの暗号／復号変換部を並列化して用いて、処理速度を２倍にすれば、平文データＡを、リアルタイムに暗号変換できるものとする。

【００３２】この場合、平文データＡはデータ領域135に書き込まれていき、暗号／復号変換部Ａ111と、暗号／復号変換部Ｂ112で、並列に暗号変換されていく。この並列暗号変換方法は前述した通りである。また、暗号文データＢ135も同時に、データ領域135に書き込まれていき、暗号／復号変換部Ｃ113で、復号変換されていく。また、鍵データ領域136には、平文データＡの暗号化に用いる鍵データＡ512と、暗号文データＢの復号化に用いる、鍵データＢ513が保存されており、初期値領域137には、平文データＡの暗号化に用いる初期値Ａ522と、暗号文データＢの復号化に用いる、初期値Ｂ523が保存されている。平文データＡ511を暗号変換するために、事前に、鍵データＡ512と初期値Ａ522を、暗号／復号変換部Ａ111と、暗号／復号変換部Ｂ112に設定し、暗号文データＢ521を復号変換するために、鍵データＢ513と初期値Ｂ523を、暗号／復号変換部Ｃ113に設定しておく。これによって、二つの、データの暗号変換および復号変換を、同時にリアルタイムで行うことが可能になる。

【００３３】次に、暗号／復号変換システム101を用いて、複数のリアルタイム・データを暗号／復号変換するための、暗号／復号変換部の管理方法について述べる。暗号／復号変換システム101を用いてリアルタイム・データの暗号変換および復号変換を行う場合、それぞれのリアルタイム・データのビットレートに合せて、使用する暗号／復号変換部の数を動的に設定することができる。これによって、効率的に、暗号／復号変換部を使用することができる。以下、この管理方法について、図面を用いて説明していく。　ここで、以下の説明において、暗号／復号変換システム101内のにはＮ個の暗号／復号変換部が並列化されているものとして一般化する。また、それぞれの暗号／復号変換部の処理速度をA[bps]とする。また、暗号／復号変換システム101の並列処理制御部117は、図６に示すような変換部管理情報330を保持している。変換部管理情報330は、未使用の暗号／復号変換部の数Ｍ331と、管理変数ｎ332と、管理テーブル340から構成される。管理テーブル340は、それぞれの暗号／復号変換部の、識別番号341と、変換するリアルタイム・データの識別番号342と、暗号／復号変換部の変換モード343と、使用状態344から成る。

【００３４】図７は、暗号／復号変換システム101の並列処理制御部117が行う、暗号／復号変換部の管理手順を示したフローチャートである。このフローチャートを元に、管理手順をステップ毎に説明していく。

【００３５】まず初めに、ステップ301で管理テーブルが初期化される。すなわち、すべての暗号／復号変換部の使用状態344を「未使用」にする。　次に、ステップ302で未使用の暗号／復号変換部の数Ｍ331に、全暗号／復号変換部数Ｎを代入する。

【００３６】次に、ステップ303で並列暗号／復号変換システムに入力される、リアルタイム・データの増減を監視する。

【００３７】まず、ステップ303で、リアルタイム・データが新たに増えた場合を説明する。この場合、まず、ステップ305でこのリアルタイム・データを処理するために使用する暗号／復号変換部の数を計算して、管理変数ｎ332に代入する。新たに入力されるリアルタイム・データのビットレートをＢ[bps]とすれば、暗号／復号変換部の数mは、以下の不等式

Ｂ　＜　ｍＡ

を満たさなければ、リアルタイムに暗号／復号変換を行うことができない。そこで、ステップ304では、使用する暗号／復号変換部の数を［Ｂ／Ａ］と定め、管理変数ｎ332に代入する。ここで、［Ｂ／Ａ］は、ＢをＡで割った結果の少数部を切り上げて整数化する演算を表す。次に、ステップ305で現在の未使用な暗号／復号変換部の数Ｍ331と管理変数ｎ332を比較し、ｎのほうが小さければ、割当て成功となり、ステップ306で管理テーブル340の変更を行う。これは以下のように処理する。まず、管理テーブル340の使用状態344を検索していき、「未使用」の暗号／復号変換部をｎ個選び出す。検索方法は、たとえば、暗号／復号変換部の識別番号341の若い順に検索していけばよい。選び出したｎ個について、識別番号342にリアルタイム・データの識別番号を設定し、リアルタイム・データを暗号変換するならモード343を「暗号」に、復号変換するなら「復号」に設定する。最後に選び出したｎ個暗号／復号変換部の使用状態344を「使用」に変更する。次に、ステップ306で未使用の暗号／復号変換部の数Ｍ331をＭ－ｎに更新する。最後に、ステップ311で、更新された管理テーブル340の各項目を元に、並列処理制御部117が、必要な暗号／復号変換部を制御して、リアルタイム・データの暗号／復号変換を開始する。

【００３８】前記ステップ305において、もし割当てが失敗したら、ステップ310で適切なエラー処理を行い、再びステップ303に戻る。エラー処理は、たとえば、必要な暗号／復号変換部がすべて、未使用になるまで待機するなどの処理を行う。以上、入力リアルタイム・デー

タが新たに増えた場合の処理について説明した。

【００３９】次に、入力リアルタイム・データが減った場合について説明する。この場合は任意のリアルタイム・データの暗号／復号変換が終了した後に、使用していた暗号／復号変換部を開放する処理を行う。まず、ステップ308で管理テーブル340の更新を行う。これは以下のように処理する。まず、管理変数ｎ332を０に初期化する。次に暗号／復号変換が終了したリアルタイム・データの識別番号を管理テーブル340から、すべて選び出す。この選択方法は、たとえば、暗号／復号変換部の識別番号の若い順に最後まで検索してけばよい。識別番号が見つかった場合、その暗号／復号変換部の使用状態344を「未使用」に変更し、管理変数ｎ332を１増やす。最後まで検索が終了すると、管理変数ｎ332には、使用していた暗号／復号変換部の数が入力されていることになる。次に、ステップ309で未使用の暗号／復号変換部の数Ｍ331をＭ＋ｎに更新し、ステップ303に戻る。以上、入力リアルタイム・データが減った場合の処理について説明した。

【００４０】上述した、本発明を用いた実施形態の説明において、暗号／復号変換システム101による、暗号および復号変換は、ＣＢＣモードを用いていたが、他の暗号運用モードを用いることも可能である。例えば、ブロック暗号方式をそのまま適用する基本モードである、ＥＣＢ(Electronic Code Book)モードを用いる場合を考える。この場合、各フレーム内の各ブロックは、独立に処理することができるので、一つのフレームから、ブロックを複数個取り出し、取り出したそれぞれのブロックを、別々の暗号／復号変換器で、同時に変換していく、ということを繰り返していくことで、並列処理を行うことができる。

【００４１】次に、本発明の他の実施形態を説明する。図８は、本発明の他の実施形態に係る、復号変換システムを内蔵した、情報処理機器の構成図である。情報処理機器800は、前記第１実施形態の情報処理機器100と同様の、外部バスインターフェイス116と、内部データ処理部118とに加えて、復号変換システム801が、内部バス171で接続された形態で構成されている。情報処理機器800は、外部バス119を介して、他の機器から暗号文データを受け取り、復号変換システム801で、復号化して、平文データを得て、内部データ処理部118でデータ処理をする機能を持っている。情報処理機器800は、機器内部で復号変換しか行わないので、復号変換システム801は、本発明の第１実施形態の暗号／復号変換システム101よりも、簡単な構成で実現できる。ような情報処理機器800の具体例として、たとえば、デジタルＴＶなどが考えられる。

【００４２】本実施形態においても、データの復号変換にＣＢＣモードを用いるとすれば、本発明の第１実施形態で説明したように、暗号／復号変換システム101で

は、フレーム単位でしか並列処理が行えなかったのに対して、復号変換システム801は、復号変換のみ行えばよいので、ブロック単位に並列処理を行うことができ、暗号／復号変換システム101に比べて、少ないメモリ容量で、並列処理できる。

【００４３】復号変換システム801は、第１実施形態の暗号／復号変換システム101と同様に、メモリ115に加えて、復号変換部Ａ811と、復号変換部Ｂ812と、復号変換部Ｃ813と、メモリ115と、並列処理制御部817とで構成される。

【００４４】復号変換部Ａ811と、復号変換部Ｂ812と、復号変換部Ｃ813は、制御部821と、変換部831で構成される。変換部831は、従来の技術で説明した、ＣＢＣモードによる復号変換を行う。

【００４５】以下、暗号／復号変換システム801が、暗号文データを復号変換する手順を図９を用いて説明していく。暗号文データ230は、データ領域135に書き込まれていき、ＣＢＣモードで復号変換を行うために、フレームに分割され、さらに各フレームは、ブロックに分割される。ここで、ブロック長は64ビットとする。従来の技術で説明したように、ＣＢＣモードにおける、暗号文ブロックの復号変換は、直前の暗号文ブロックをを用いるだけでよいので、暗号変換のように、変換したブロックを、フィードバックする必要がない。したがって、同一フレーム内でも、直前の暗号文ブロックを参照できれば、ブロック単位に独立に復号変換を行うことができる。

【００４６】図９においては、暗号文データは、暗号文フレームＡ231、暗号文フレームＢ232、暗号文フレームＣ233、...というようにフレーム分割される。暗号文フレームＡ231は、暗号文ブロックＣ[1]251、暗号文ブロックＣ[2]252、暗号文ブロックＣ[3]253、...暗号文ブロックＣ[n]258とn個のブロックに分割される。ここで、最後の暗号文ブロックＣ[n]258の長さが、64ビット未満の場合は、端数暗号文ブロックとして区別しておく。暗号ブロックが、順番にデータ領域135に書き込まれていくと、復号変換部Ａ811は、暗号文ブロックC[1]251と、初期値領域から、初期値を読み込み、復号変換して、平文ブロックM[1]をデータ領域135に書きむ。復号変換部Ｂ812は、暗号文ブロックC[2]252と、暗号文ブロックC[2]251を読み込み、復号変換して、平文ブロックM[2]をデータ領域135に書きむ。同様に、復号変換部Ｃ812は、暗号文ブロックC[3]253と、暗号文ブロックC[2]252を読み込み、復号変換して、平文ブロックM[3]をデータ領域135に書きむ。以上のような暗号ブロックの復号化を、復号変換部Ａ811と、復号変換部Ｂ812と、復号変換部Ｃ813が、最後のブロックまで、並列に処理していく。これによって、同一フレーム内での、並列復号変換を行うことが可能になる。この並列処理の制御は、並列処理制御部817が行い、それぞれの復号変換部が、どの

暗号文ブロックを復号変換すればよいかを指示していく。

【００４７】次に、本実施例の変換部831の内部構造について、詳細に説明する。

【００４８】図１０は、変換部831の詳細構成図であり、以下のモジュールより構成される。1011は２入力マルチプレクサ、1012は３入力マルチプレクサ、431は排他的論理和演算部、441はブロック暗号部である。上記モジュールの入力および出力は、すべて64ビットのパラレル入出力である。ブロック暗号部441は、第１実施形態で説明したものと同様である。

【００４９】まず、一番先頭の暗号文ブロックの復号変換を考える。この場合、変換部431には暗号文ブロックＣ[1]と、初期値と、鍵データが入力さる。暗号文Ｃ[1]はマルチプレクサ1011を介して、ブロック暗号部441に入力され、鍵データを用いて、復号変換される。ここで、ブロック暗号部441は復号モードに設定する。ブロック暗号部441からの出力は、排他的論理輪演算部431に入力される。一方で、初期値がマルチプレクサ1012を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値が、平文ブロックM[1]となる。

【００５０】次に、2からn-1の間の任意の整数をkとし、k番目の暗号文ブロックの復号変換を考える。この場合、変換部431には暗号文ブロックC[k]とその直前の暗号文ブロックC[k-1]と、鍵データが入力される。暗号文ブロックＣ[k]はマルチプレクサ1011を介して、ブロック暗号部441に入力され、鍵データを用いて、復号変換される。ここで、ブロック暗号部441は復号モードに設定する。ブロック暗号部441からの出力は、排他的論理輪演算部431に入力される。一方で、暗号文ブロックＣ[k-1]がマルチプレクサ1012を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値が、平文ブロックM[k]となる。

【００５１】次に、ｎ番目すなわち最後の暗号文ブロックの復号変換を考える。この場合、変換部431には、暗号文ブロックC[n]とその直前の暗号文ブロックC[n-1]と、鍵データが入力される。

【００５２】まず、暗号文ブロックC[n]が、端数暗号文ブロックである場合は、以下のように端数処理を行う。暗号文ブロックＣ[n]はマルチプレクサ1012を介して、排他的論理輪演算部431に入力される。一方で、暗号文ブロックＣ[n-1]がマルチプレクサ1011を介して、ブロック暗号部441に入力され、鍵データを用いて、暗号変換される。ここで、ブロック暗号部441は暗号モードに設定する。ブロック暗号部441からの出力は、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値が、平文ブロックM[n]となる。

【００５３】次に暗号文ブロックC[n]が、端数ブロックでなければ以下のように変換を行う。暗号文ブロックＣ[n]はマルチプレクサ1011を介して、ブロック暗号部441に入力され、鍵データを用いて、復号変換される。ここで、ブロック暗号部441は復号モードに設定する。ブロック暗号部441からの出力は、排他的論理輪演算部431に入力される。一方で、暗号文ブロックＣ[n-1]がマルチプレクサ1012を介して、排他的論理和演算部431に入力される。排他的論理和演算部431の出力値が、平文ブロックM[n]となる。

【００５４】以上の処理によって、変換部431は、暗号文ブロック列を、暗号文ブロック列に暗号変換していくことができる。ここで、マルチプレクサのスイッチング、ブロック暗号部の暗号および復号モードの設定は、制御部821が行う。

【００５５】上述した実施形態の説明において、復号変換システム801による、復号変換は、ＣＢＣモードを用いていたが、他の暗号運用モードを用いることも可能である。例えば、ブロック暗号方式をそのまま適用する基本モードである、ＥＣＢ(Electronic Code Book)モードを用いる場合を考える。この場合、各フレーム内の各ブロックは、独立に処理することができるので、一つのフレームから、ブロックを複数個取り出し、取り出したそれぞれのブロックを、別々の復号変換器で、同時に変換していく、ということを繰り返していくことで、並列処理を行うことができる。

【００５６】次に、本発明の他の実施形態を説明する。図１１は、本発明の他の実施形態に係る、暗号／復号変換システムを内蔵した、情報処理機器の構成図である。情報処理機器1100は、前記第１実施形態の情報処理機器100と同様の、外部バスインターフェイス116と、内部データ処理部118とに加えて、暗号／復号変換システム1101が、内部バス171で接続された形態で構成されている。

【００５７】暗号／復号変換システム1101は、ＣＰＵ1101と、メモリ1115とで構成される。ＣＰＵ1101は、実行部Ａ1111と、実行部Ｂ1112と、実行部Ｃ1113と、命令部1121と、レジスタ部1130が、内部ＣＰＵバス1141で接続されている構成で、３本のパイプラインをもつ、スーパースカラ方式のＣＰＵである。ここで、スーパースカラ方式とは、複数の実行部を備えることで、１クロック・サイクル当たり、複数の独立した命令を同時に実行することができる方式である。

【００５８】メモリ1115は、前記第１実施形態のメモリ115と同様の、データ領域135と、鍵データ領域136と、初期値領域137とに加えて、プログラム領域1181に分割される。プログラム領域1181には、ＣＰＵ1101で暗号／復号変換を行うための、制御プログラムが格納される。

【００５９】この制御プログラムは、ＲＯＭ、Floppy disk、または、ネットワークを介して本システムに接続されたサーバ上の記憶装置から取り込まれることがある。

【００６０】レジスタ部1130内には、レジスタＡ1131と、レジスタＢ1132と、レジスタＣ1133が含まれ、それ

ぞれ１個以上のレジスタから構成される、このような、情報処理機器1100の具体例として、パーソナルコンピューターなどが考えられる。

【００６１】データ領域135には、暗号／復号変換システム101外部から、暗号あるいは復号変換を行いたいデータが、順次、書き込まれてくる。一方、プログラム領域に格納されている、制御プログラムをＣＰＵ1110の命令部1121が、順次読み込んで実行していく。制御プログラムは、データ領域135に書き込まれてくるデータを、レジスタ部1130のレジスタＡ1131と、レジスタＢ1132と、レジスタＣ1133に、読み込んで、実行部Ａ1111と、実行部Ｂ1112と、実行部Ｃ1113を、並列に用いて、暗号あるいは復号変換させ、その結果を再び、データ領域135に書き込んでいくように、プログラムされている。これによって、データ領域135内のデータが暗号あるいは復号変換処理されていく。データ領域135内の暗号あるいは復号変換処理されたデータは、順次、暗号／復号変換システム1101外部に読み出されていく。

【００６２】以下、暗号／復号変換システム1101が、具体的にはＣＰＵ1110が制御プログラムを実行し、平文データを暗号変換する手順を図１２を用いて説明していく。第１実施例の暗号／復号変換システム101と同様に、平文データ220は、データ領域135に書き込まれ、暗号変換を行うために、フレームに分割され、さらにブロックに区切られていく。次に、平文フレームＡ221の、先頭の平文ブロックを、レジスタＡ1131に読み込み、続いて、平文フレームＢ222の、先頭の平文ブロックを、レジスタＢ1132に読み込み、続いて、平文フレームＣ223の、先頭の平文ブロックを、レジスタＣ1133に読み込む。レジスタＡ1131およびレジスタＢ1132およびレジスタＣ1133に読み込まれた平文ブロックは、すべて独立であり、かつ、同じ暗号変換処理を行ことになる。したがって、ＣＰＵ内の制御部1141が、レジスタＡの暗号変換処理に実行部Ａ1111を割当てて、レジスタＢの暗号変換処理に実行部Ｂ1111を割当てて、レジスタＣの暗号変換処理に実行部Ｃ1111を割当る。これによって、レジスタＡ1131とレジスタＢ1132とレジスタＣ1133の処理を、３本のパイプラインを用いて並列実行することができる。暗号変換処理が終了すると、それぞれのレジスタの値を、データ領域135の同じ場所に書きこみ、先頭の暗号文ブロックが生成される。これを、以降の平文ブロックに対しても、行っていくことで、平文フレームＡ221と、平文フレームＢ222と、平文フレームＣ223を、暗号文フレームＡ231と、暗号文フレームＢ232と、暗号文フレームＣ233に、並列に、暗号変換していく。同様な処理を、他の平文フレームでも行っていくことで、平文データ220の暗号変換を、並列処理することができる。

【００６３】次に、暗号／復号変換システム1101が、具体的にはＣＰＵ1110が制御プログラムを実行し、暗号文データを復号変換する手順を図１３を用いて説明していく。前述の実施例の復号変換システム801と同様に、暗号文データ230は、データ領域135に書き込まれていき、復号変換を行うために、フレームに分割され、さらに各フレームは、ブロックに分割される。図１３においては、暗号文フレームＡ231が、暗号文ブロックC[1]251から暗号文ブロックC[n]258に分割される。

【００６４】まず、レジスタＡ1131は、初期値領域から、初期値を読み込み、続いて、データ領域135から暗号文ブロックC[1]251を読み込みこむ。次にレジスタＢ1132は、データ領域135から、暗号文ブロックC[2]252と、暗号文ブロックC[2]251を読み込む。次に、レジスタＣ1133は、データ領域135から、暗号文ブロックC[3]253と、暗号文ブロックC[2]252を読み込む。レジスタＡ1131およびレジスタＢ1132およびレジスタＣ1133の処理は、すべて独立であるので、ＣＰＵ内の制御部1141が、レジスタＡの暗号変換処理に実行部Ａ1111を割当てて、レジスタＢの暗号変換処理に実行部Ｂ1111を割当てて、レジスタＣの暗号変換処理に実行部Ｃ1111を割当る。これによって、レジスタＡ1131とレジスタＢ1132とレジスタＣ1133の処理を、３本のパイプラインを用いて並列実行することができる。暗号変換処理が終了すると、それぞれのレジスタの値を、データ領域135に書きこんでいく。レジスタＡ1131からは、平文ブロックM[1]が得られ、レジスタＢ1132からは、平文ブロックM[2]が得られ、レジスタＣ1133からは、平文ブロックM[3]が得られる。

【００６５】同様な処理を、以降の暗号文ブロックについても行っていくことで、暗号文フレーム231の復号変換を、並列処理することができる。さらに、他の暗号文フレームに対しても、同様な処理を行うことで、暗号文データ230を並列に平文データ220に変換できる。

【００６６】次に、暗号／復号変換システム1101が、並列に暗号／復号変換を行うための、メモリ1115のプログラム領域1181に格納される、制御プログラムの構成について、説明していく。

【００６７】図１４は、暗号変換の制御を行う暗号変換プログラム1203、および復号変換の制御を行う復号変換プログラム1213の生成手順を表している。暗号変換プログラム1203、および復号変換プログラム1213は、機械語であるので、暗号変換プログラム1203を生成するには、プログラム言語で書かれた、ソースコード1201を、コンパイラ1202でコンパイルする。同様に、復号変換1213を生成するには、ソースコード1211を、コンパイラ1202でコンパイルする必要がある。

【００６８】次に、並列に暗号変換を行うためのソースコード1201の構成を説明する。まず、並列に暗号変換を行わない、通常の処理手順を記述した、ソースコードを図１５に示す。前述したように、暗号変換はフレーム毎に行われる。それぞれのフレームの暗号変換処理は、複数の処理手順に分割されるが、それぞれの処理手順は、

相関があるので、並列に処理することはできない。図１５において、処理Ａ１(1311)、処理Ａ２(1312)、処理Ａ３(1313)、...は、フレームＡの暗号変換処理を表している。また、処理Ｂ１(1321)、処理Ｂ２(1322)、処理Ｂ３(1323)、...は、フレームＢの暗号変換処理を表している。また、処理Ｃ１(1311)、処理Ｃ２(1312)、処理Ｃ３(1313)、...は、フレームＣの暗号変換処理を表している。図１３のソースコードのように、まず、フレームＡを処理し、次にフレームＢを処理し、次にフレームＣを処理し、...というように、処理を記述していくと、全体の暗号変換処理は、並列化されない。次に、並列に暗号変換を行うように記述された、ソースコードを図１６に示す。図１６のソースコードは、まず、フレームＡの処理Ａ１(1311)と、フレームＢの処理Ｂ１(1321)と、フレームＣの処理Ｃ１(1331)を実行し、次に、フレームＡの処理Ａ２(1312)と、フレームＢの処理Ｂ２(1322)と、フレームＣの処理Ｃ２(1332)を実行し、次に、フレームＡの処理Ａ３(1313)と、フレームＢの処理Ｂ３(1323)と、フレームＣの処理Ｃ３(1333)を実行し、...というように、記述されている。このように記述すると、処理Ａ１(1311)と、処理Ｂ１(1321)と、処理Ｃ１(1331)は独立であるので、並列に実行され、処理Ａ２(1312)と、処理Ｂ２(1322)と、処理Ｃ２(1332)は独立であるので、並列に実行され、...というように、暗号変換を並列に処理していくことが可能になる。

【００６９】次に、並列に復号変換を行うためのソースコード1211の構成を説明する。まず、並列に復号変換を行わない、通常の処理手順を記述した、ソースコードを図１７に示す。前述したように、復号変換はブロック毎に行われる。それぞれのブロックの復号変換処理は、複数の処理手順に分割されるが、それぞれの処理手順は、相関があるので、並列に処理することはできない。図１５において、処理ａ１(1511)、処理ａ２(1512)、処理ａ３(1513)、...は、ブロックａの復号変換処理を表している。また、処理ｂ１(1521)、処理ｂ２(1522)、処理ｂ３(1523)、...は、ブロックｂの復号変換処理を表している。また、処理ｃ１(1511)、処理ｃ２(1512)、処理ｃ３(1513)、...は、ブロックｃの復号変換処理を表している。図１７のソースコードのように、まず、ブロックａを処理し、次にブロックｂを処理し、次にブロックｃを処理し、...というように、処理を記述していくと、全体の復号変換処理は、並列化されない。次に、並列に復号変換を行うように記述された、ソースコードを図１８に示す。図１８のソースコードは、まず、ブロックａの処理ａ１(1511)と、ブロックｂの処理ｂ１(1521)と、ブロックｃの処理ｃ１(1531)を実行し、次に、ブロックａの処理ａ２(1512)と、ブロックｂの処理ｂ２(1522)と、ブロックｃの処理ｃ２(1532)を実行し、次に、ブロックａの処理ａ３(1513)と、ブロックｂの処理ｂ３(1523)と、ブロックｃの処理ｃ３(1533)を実行し、...というように、記述されている。このように記述すると、処理ａ１(1511)と、処理ｂ１(1521)と、処理ｃ１(1531)は独立であるので、並列に実行され、処理ａ２(1512)と、処理ｂ２(1522)と、処理ｃ２(1532)は独立であるので、並列に実行され、...というように、復号変換を並列に処理していくことが可能になる。

【００７０】上述した、実施形態の説明において、暗号／復号変換システム1001による、暗号および復号変換は、ＣＢＣモードを用いていたが、他の暗号運用モードを用いることも可能である。例えば、ブロック暗号方式をそのまま適用する基本モードである、ＥＣＢ(Electronic Code Book)モードを用いる場合を考える。この場合、各フレーム内の各ブロックは、独立に処理することができるので、一つのフレームから、ブロックを複数個取り出し、取り出したそれぞれのブロックを、ＣＰＵ1101内の別々の実行部で、同時に変換していく、ということを繰り返していくことで、並列処理を行うことができる。

【００７１】次に、本発明の他の実施形態として、ＤＶＤ (Digital Video Disc) などのパッケージコンテンツを流通させるシステムの実施例を図１９に示す。

【００７２】コンテンツプロバイダー1401は、著作権管理機関1418に著作権情報を登録し、コンテンツID情報IDA 1402を得る。IDAはデジタルデータにID情報などを隠しもたせる技術である電子透かしを用いてコンテンツデータ1403に埋め込まれ、パッケージコンテンツ1404となる。ここで、図２０はパッケージコンテンツ1404内のコンテンツデータを表しており、コンテンツ情報IDA 1402が電子透かしとして含まれている。

【００７３】情報家電B 1405がパッケージコンテンツ1404内のコンテンツデータをパーソナルコンピュータC 1411に転送する場合、情報家電B 1405は著作権管理機関1419から発行されたユーザID情報IDB 1407を電子透かしとしてコンテンツデータ内に埋め込み、本発明を用いた暗号装置1406で鍵データK 1408により暗号化し、外部バス上に暗号データを流す。図２１は経路1409を流れるコンテンツデータを表しており、コンテンツ情報IDA 1402およびユーザID情報IDB 1407が電子透かしとして含まれている。

【００７４】受信側であるパーソナルコンピュータC 1411は、暗号データを、本発明を用いた復号装置1413で鍵データK 1415により復号化する。以上の処理において、ユーザ情報や鍵データの管理にICカード1410を用いてもよい。

【００７５】パーソナルコンピュータC 1411がネットワーク上にコンテンツデータを流通させる場合、パーソナルコンピュータC 1411は著作権管理機関1419から発行されたユーザID情報IDC 1414を電子透かしとしてコンテンツデータ内に埋め込み、本発明を用いた暗号装置1410で、データを鍵データK 1415により暗号化する。

図２２は経路1409を流れるコンテンツデータを表しており、コンテンツ情報IDA　1402、ユーザID情報IDB　1407およびユーザID情報IDC　1414が電子透かしとして含まれている。以上の処理において、ユーザ情報や鍵データの管理にICカード1417を用いてもよい。

【００７６】著作権管理機1419は、検査装置1419を用いて、ネットワーク上を流れるデータを監視し、暗号化されていないデータを検出した場合、データ内のコンテンツID情報を著作権情報管理データベース1420と照合し、不正コピーと判断すれば、不正コピーの発生場所をユーザID情報から追跡し、ペナルティを課す。

【００７７】また、本発明を用いたデジタル衛星放送などのデジタルコンテンツの流通システムの実施例を図２３に示す。コンテンツプロバイダー1401は、著作権管理機関1418に著作権情報を登録し、コンテンツID情報IDA　1402を得る。IDAを電子透かしとして埋め込んだコンテンツデータ1403は、放送センタ1801に送られ、既存の暗号装置1802で暗号化され、デジタル衛星放送受信機などの情報家電に向けて放送される。情報家電は既存の復号化装置1803で放送データを復号化する。情報家電には、既存の復号装置1803に加えて本発明を用いた暗号装置1406を備えており、その後のコンテンツデータの流通過程は図１９における例と同様に行うことができる。

【００７８】このように、デジタル衛星放送などの既存の暗号システムと本発明の暗号システムを組み合わせて、デジタルコンテンツの流通システムを構築することも可能であり、パッケージメディア、放送メディア、通信メディアと幅広く本発明の適用が可能である。

【００７９】

【発明の効果】本発明によれば、データの暗号変換を、または復号変換をそれぞれ高速に処理することができる。

【図面の簡単な説明】

【図１】本発明を用いた、情報処理機器の第１実施例である。

【図２】第１実施例における、暗号変換手順の詳細図である。

【図３】第１実施例における、復号変換手順の詳細図である。

【図４】図１における、変換部の詳細図である。

【図５】図１における、情報処理機器が、暗号変換と、復号変換を同時に行う場合の概要図である。

【図６】図１における、暗号／復号変換システムで、複数のデータを、リアルタイムに、暗号／復号変換するために用いる管理情報の詳細図である。

【図７】図１における、暗号／復号変換システムで、複数のデータを、リアルタイムに、暗号／復号変換するための、管理手順ののフローチャートである。

【図８】本発明を用いた、情報処理機器の他の実施例で＊ある。

【図９】他の実施例における、復号変換手順の詳細図である。

【図１０】図８における、変換部の詳細図である。

【図１１】本発明を用いた、情報処理機器の他の実施例である。

【図１２】他の実施例における、暗号変換手順の詳細図である。

【図１３】他の実施例における、復号変換手順の詳細図である。

【図１４】制御プログラムの、生成手順の概要図である。

【図１５】暗号変換を行うように記述された、ソースコードの概念図（その１）である。

【図１６】暗号変換を行うように記述された、ソースコードの概念図（その２）である。

【図１７】復号変換を行うように記述された、ソースコードの概念図（その１）である。

【図１８】復号変換を行うように記述された、ソースコードの概念図（その２）である。

【図１９】本発明を用いたパッケージコンテンツの流通システムに関する一実施例である。

【図２０】電子透かしを含むコンテンツデータ（その１）である。

【図２１】電子透かしを含むコンテンツデータ（その２）である。

【図２２】電子透かしを含むコンテンツデータ（その３）である。

【図２３】本発明を用いた放送コンテンツの流通システムに関する一実施例である。

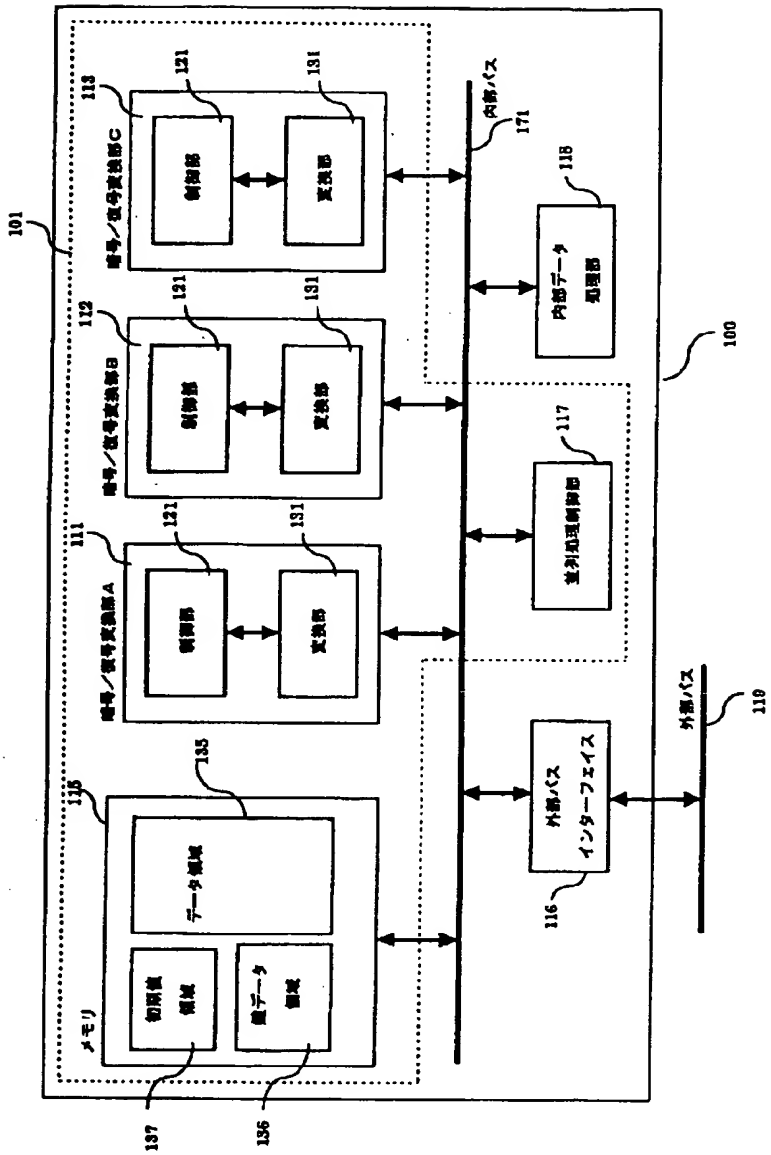
【図２４】ＣＢＣモードによる、暗号変換および復号変換の処理手順の詳細図である。

【符号の説明】

100…情報処理機器、
101…暗号／復号変換システム、
111…暗号／復号変換部Ａ、
112…暗号／復号変換部Ｂ、
113…暗号／復号変換部Ｃ、
115…メモリ、
116…外部バスインターフェイス、
117…並列処理制御部、
118…内部データ処理部、
119…外部バス、
121…制御部、
131…変換部、
135…データ領域、
136…鍵データ領域、
137…初期値領域、
171…内部バス。

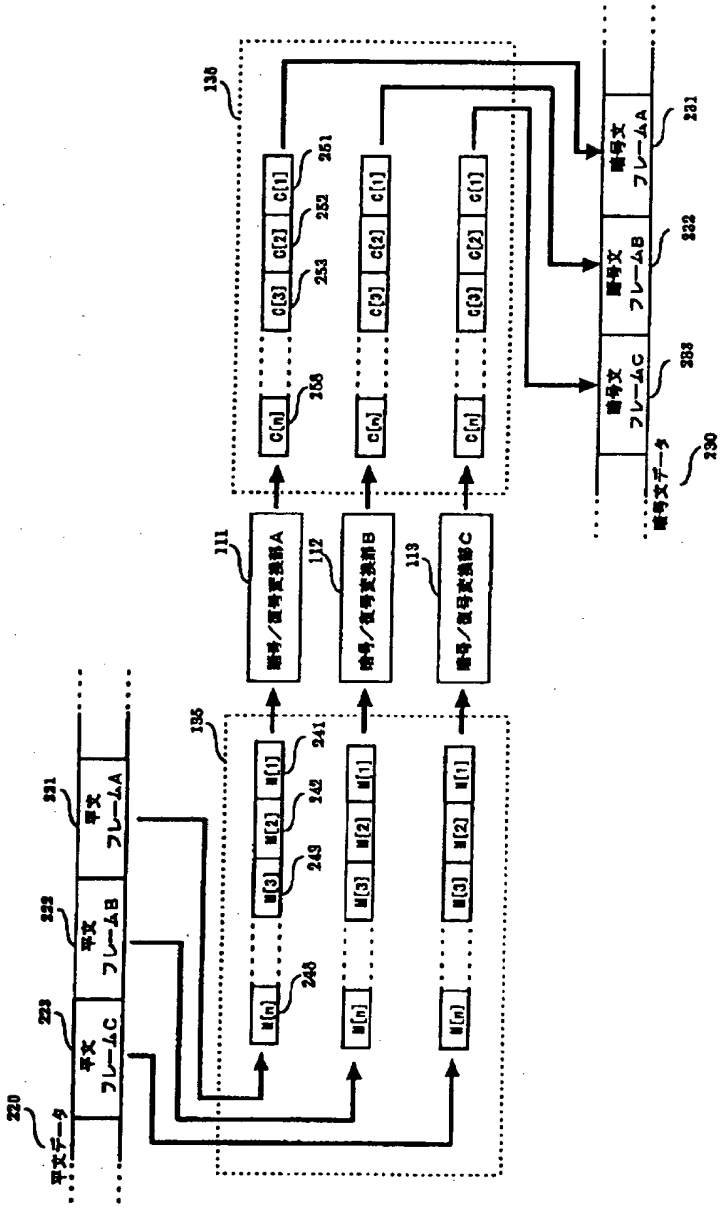
【図１】

図　１


101
100
113
121
131
符号／復号変換部C
制御部
変換部
112
符号／復号変換部B
111
符号／復号変換部A
内部バス
171
118
内部データ処理部
117
並列処理制御部
外部バス
インターフェイス
116
外部バス
110
135
データ領域
136
データ領域
137
初期値領域
メモリ

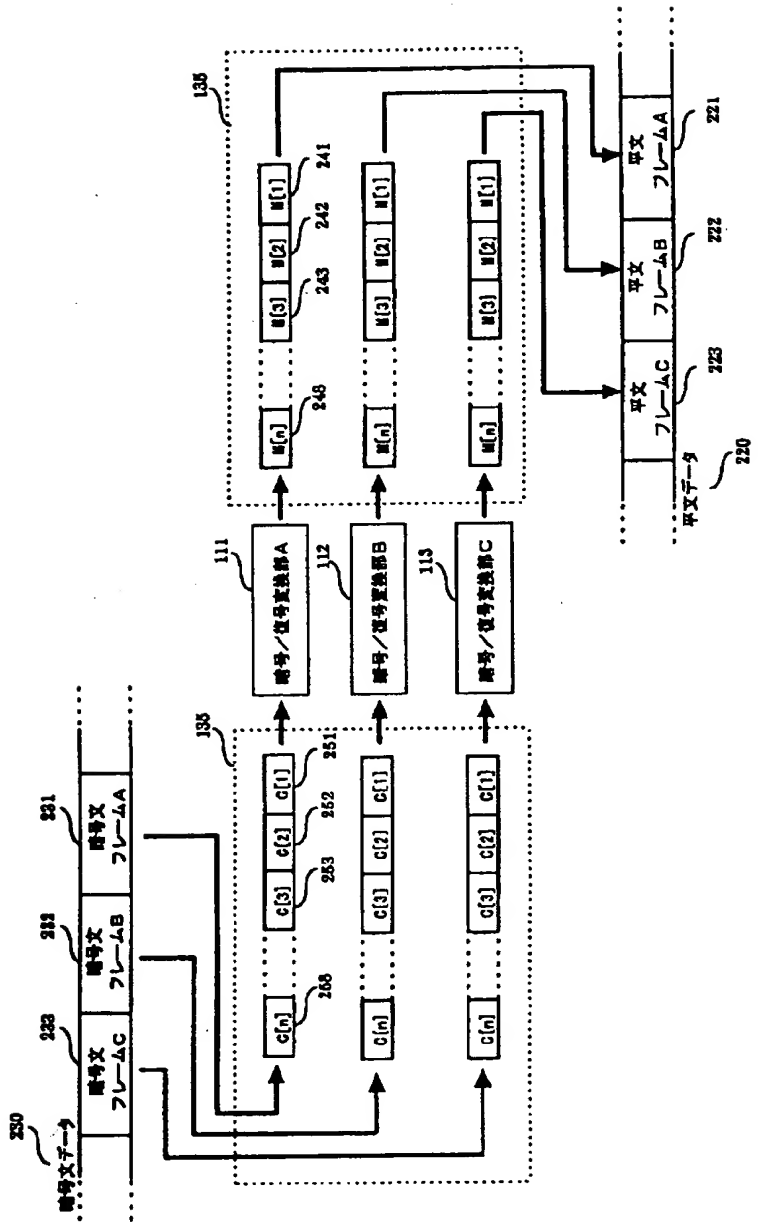
【図２】

図　２


平文データ
220
平文 フレームA
221
平文 フレームB
222
平文 フレームC
223
暗号／復号変換部A
111
暗号／復号変換部B
112
暗号／復号変換部C
113
暗号文 フレームA
231
暗号文 フレームB
232
暗号文 フレームC
233
暗号文データ
230
130
135
C[1]
C[2]
C[3]
C[n]
M[1]
M[2]
M[3]
M[n]

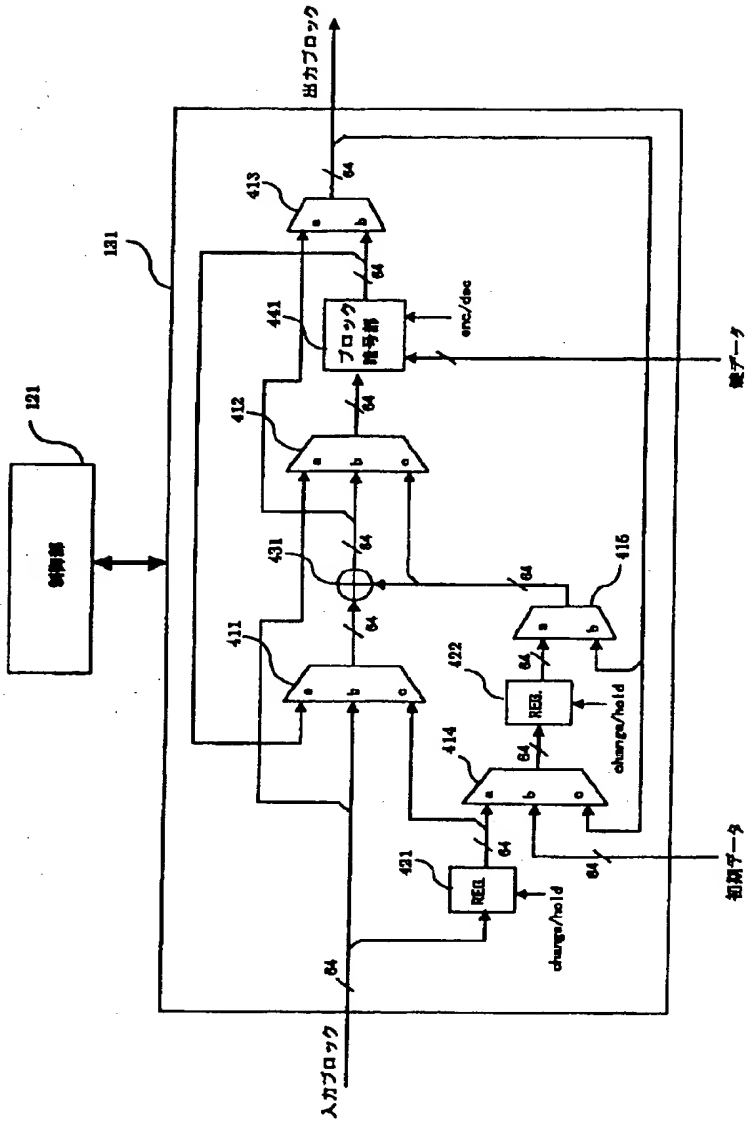
【図３】

図　３


暗号文データ
暗号文 フレームC
暗号文 フレームB
暗号文 フレームA
暗号／復号変換部A
暗号／復号変換部B
暗号／復号変換部C
平文データ
平文 フレームC
平文 フレームB
平文 フレームA

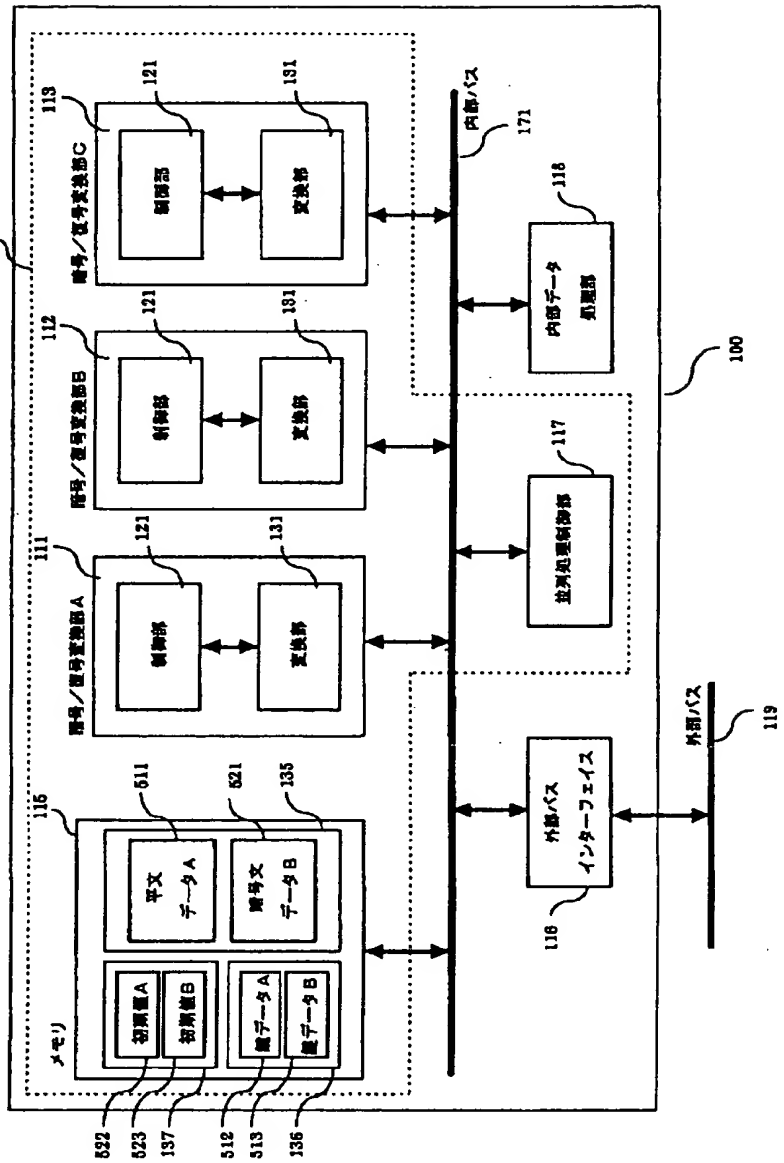
【図４】

図　4


出力ブロック
413
64
131
441
ブロック
保持部
enc/dec
復データ
121
412
431
411
416
422
REG
change/hold
414
421
初期データ
入力ブロック
制御部

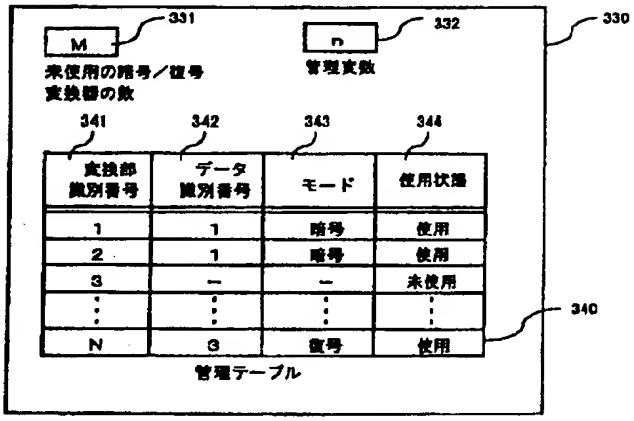
【図５】

図　５


101
100
111
112
113
121
131
暗号／復号変換部A
暗号／復号変換部B
暗号／復号変換部C
制御部
変換部
内部バス
171
内部データ処理部
118
117
並列処理制御部
外部バス
インターフェイス
116
119
メモリ
511
521
135
平文データA
暗号文データB
初期値A
初期値B
鍵データA
鍵データB
522
523
137
512
513
136

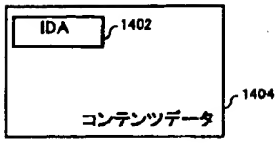
【図６】

図　6



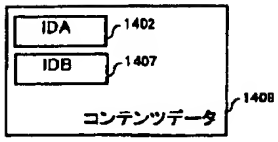
【図２０】

図　20



【図２１】

図　21



【図１０】

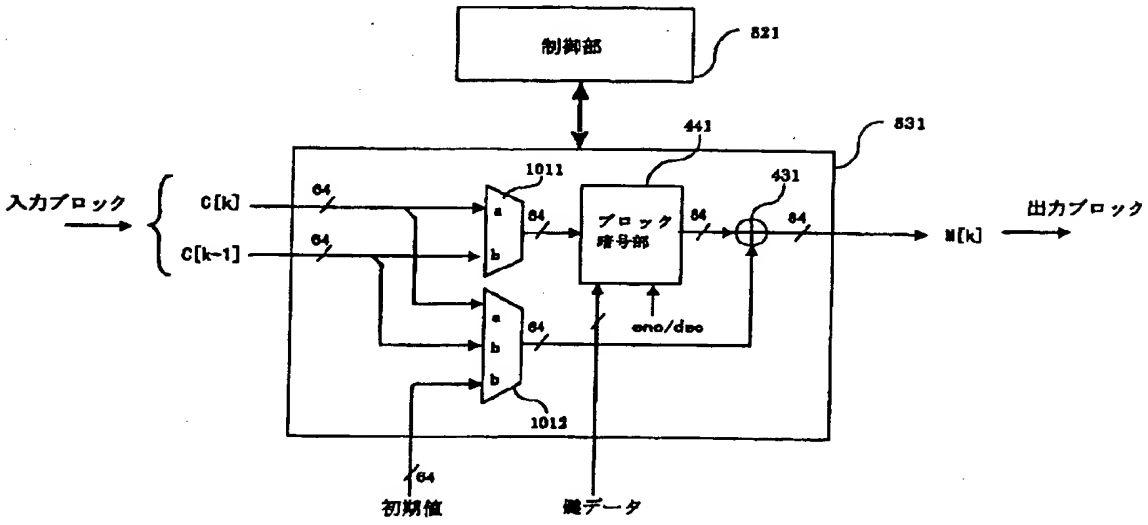
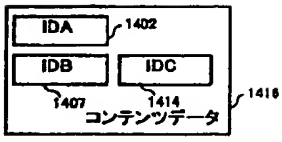


図　10

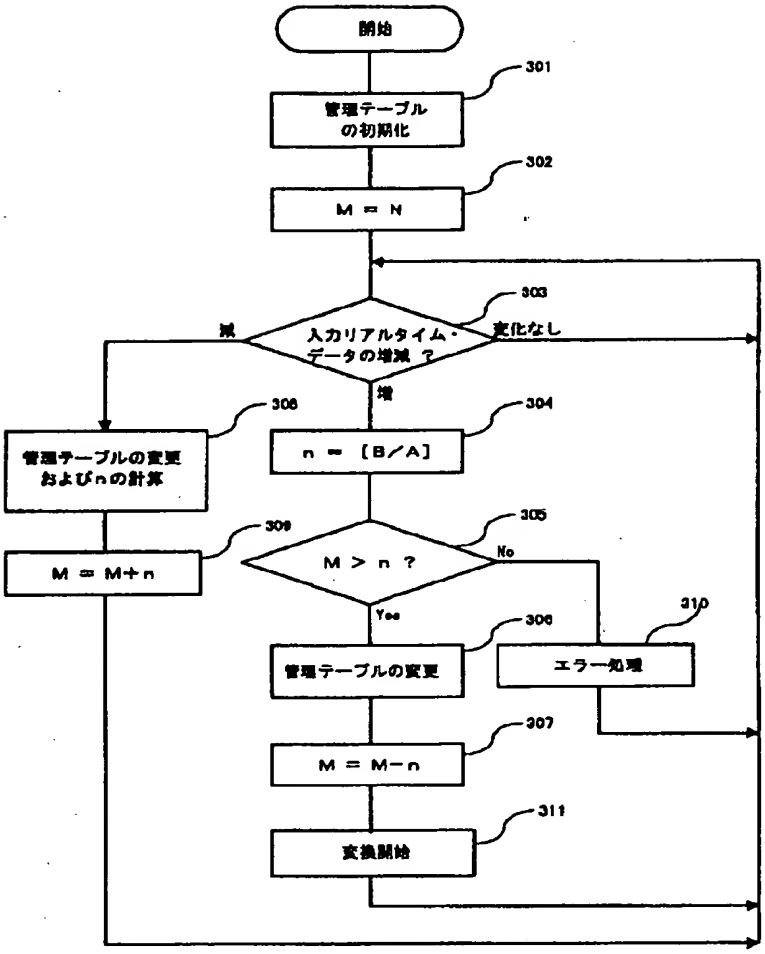
【図２２】

図　22



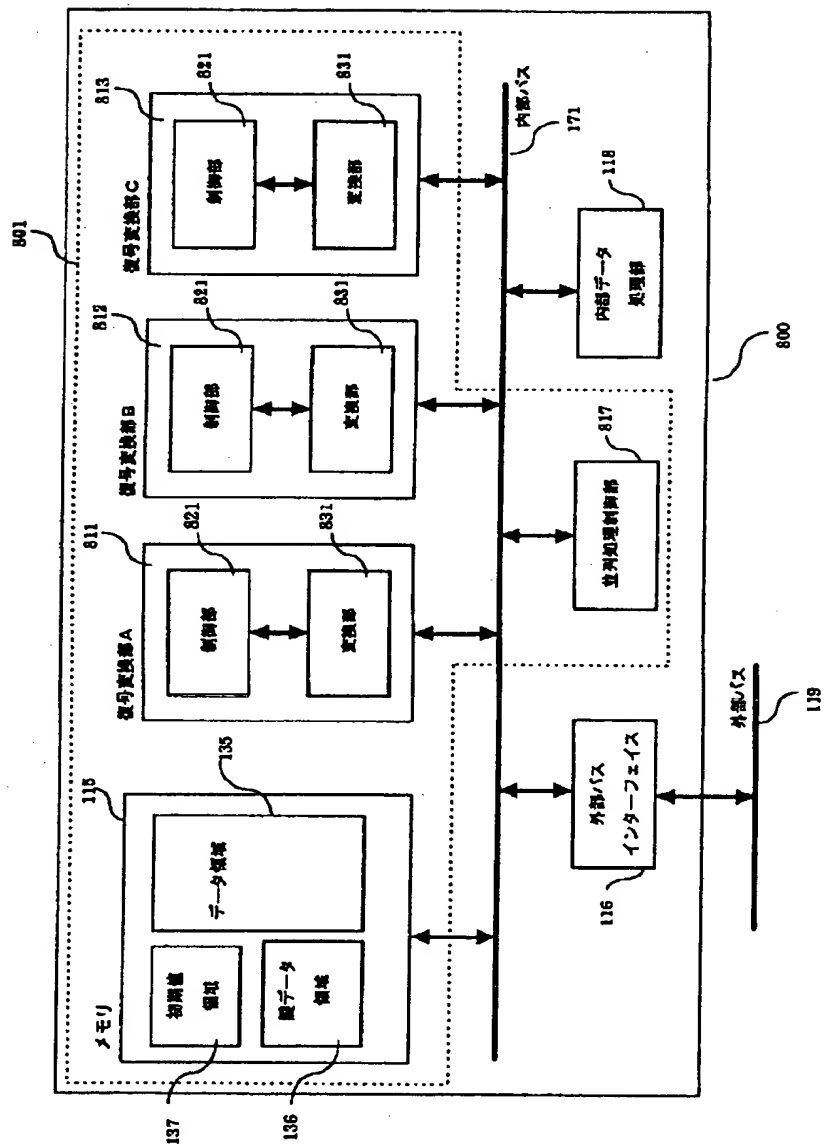
【図７】

図　7


開始
301
管理テーブル
の初期化
302
M = N
303
入力リアルタイム・
データの増減 ?
減
変化なし
増
306
管理テーブルの変更
およびnの計算
304
n = 〔B／A〕
309
M = M+n
305
M > n ?
No
Yes
310
306
管理テーブルの変更
エラー処理
307
M = M−n
311
変換開始

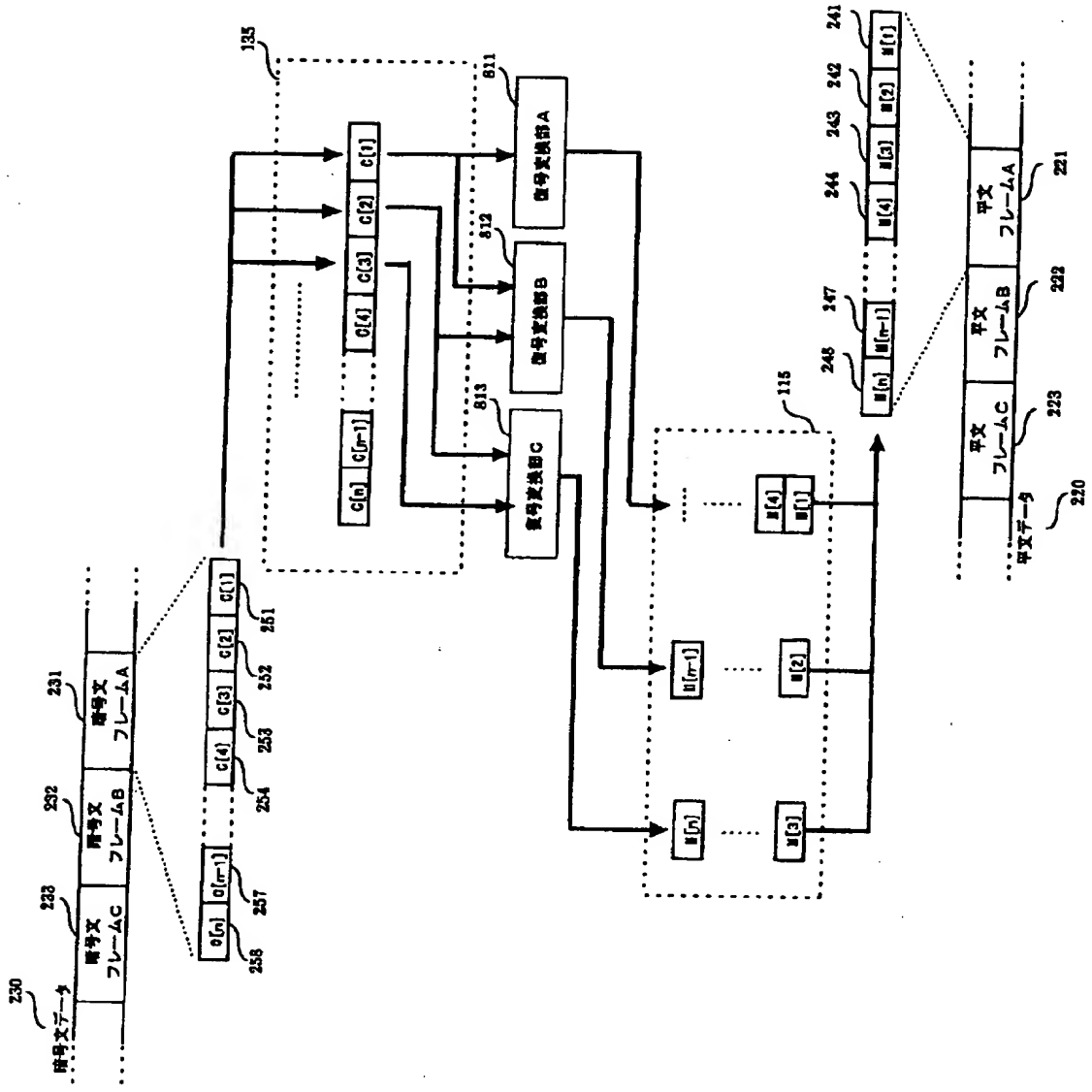
【図８】

図 8


801
813
821
831
制御部
変換部
復号変換部C
812
821
831
制御部
変換部
復号変換部B
811
821
831
制御部
変換部
復号変換部A
内部バス
171
118
内部データ処理部
800
817
並列処理制御部
外部バス
インターフェイス
116
外部バス
119
115
135
データ領域
初期値領域
誤データ領域
メモリ
137
136

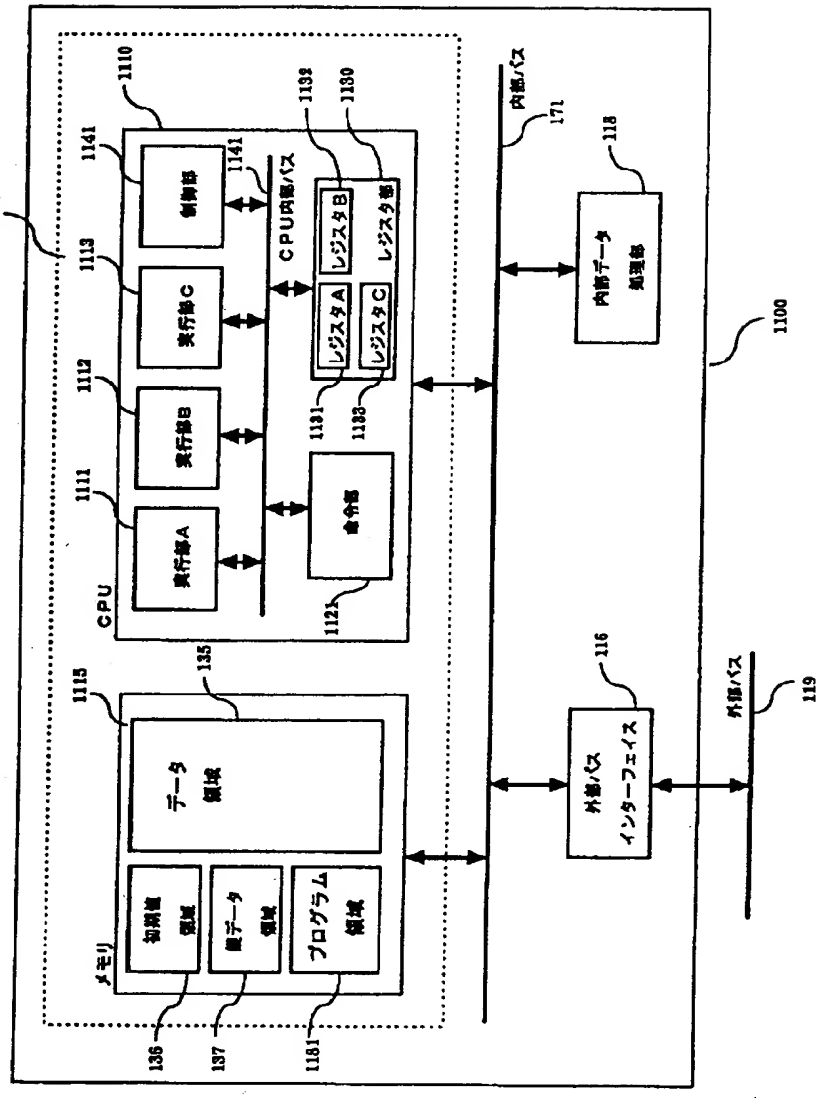
【図９】

図　９


135
811
812
813
115
241
242
243
244
247
248
231
232
233
230
221
222
223
220
暗号文データ
暗号文 フレームA
暗号文 フレームB
暗号文 フレームC
平文 フレームA
平文 フレームB
平文 フレームC
平文データ
暗号変換部A
暗号変換部B
暗号変換部C

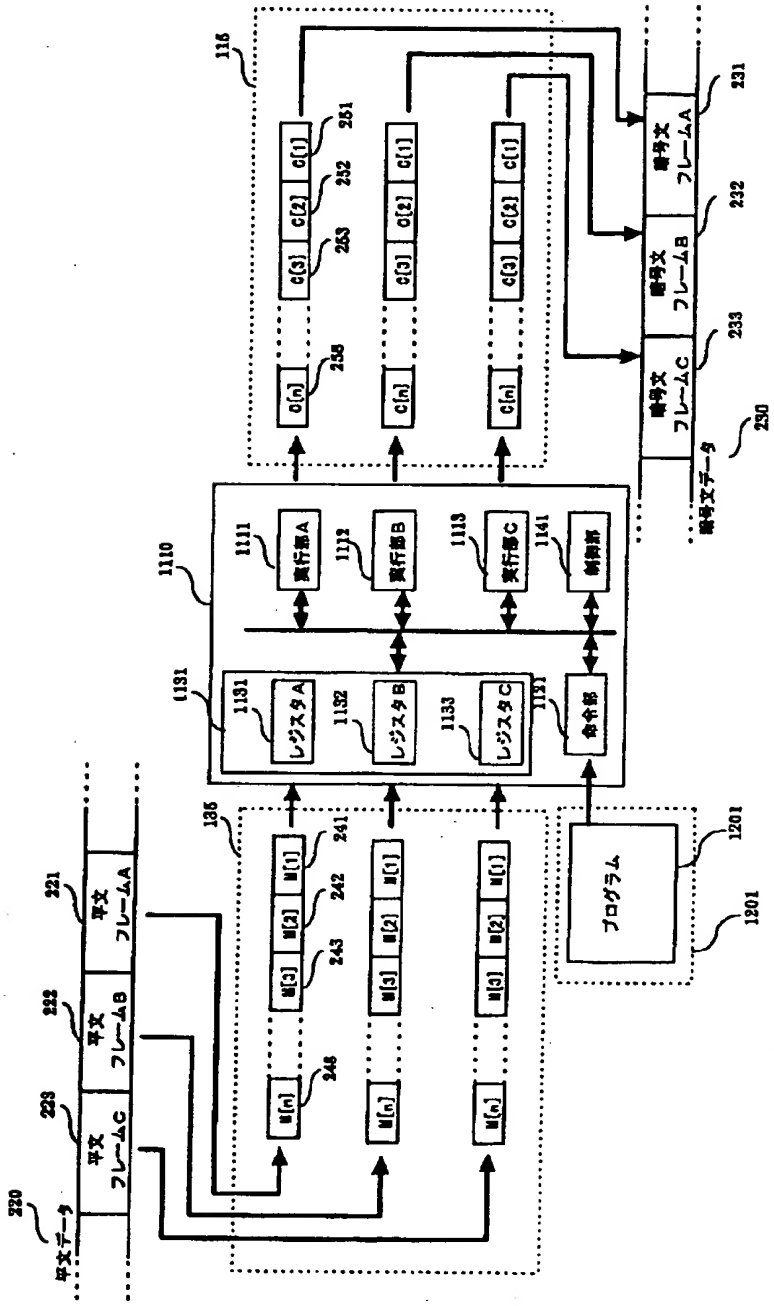
【図１１】

図　１１


1101
1110
1141
制御部
1113
実行部C
1112
実行部B
1111
実行部A
CPU
1121
CPU内部バス
1133
1130
レジスタB
レジスタA
レジスタC
レジスタ部
1131
1133
内部バス
171
118
内部データ処理部
1100
116
外部バスインターフェイス
外部バス
119
1115
135
データ領域
初期値領域
固定データ領域
プログラム領域
メモリ
136
137
1181

【図１２】

図　１２


116
251
252
253
255
c[1]
c[2]
c[3]
c[n]
231
232
233
250
暗号文 フレームA
暗号文 フレームB
暗号文 フレームC
暗号文データ
1110
1111
1112
1113
1141
実行部A
実行部B
実行部C
制御部
1131
1131
1132
1133
1151
レジスタA
レジスタB
レジスタC
命令部
136
241
242
243
245
M[1]
M[2]
M[3]
M[n]
1201
1301
プログラム
220
221
222
223
平文データ
平文 フレームA
平文 フレームB
平文 フレームC

【図１３】

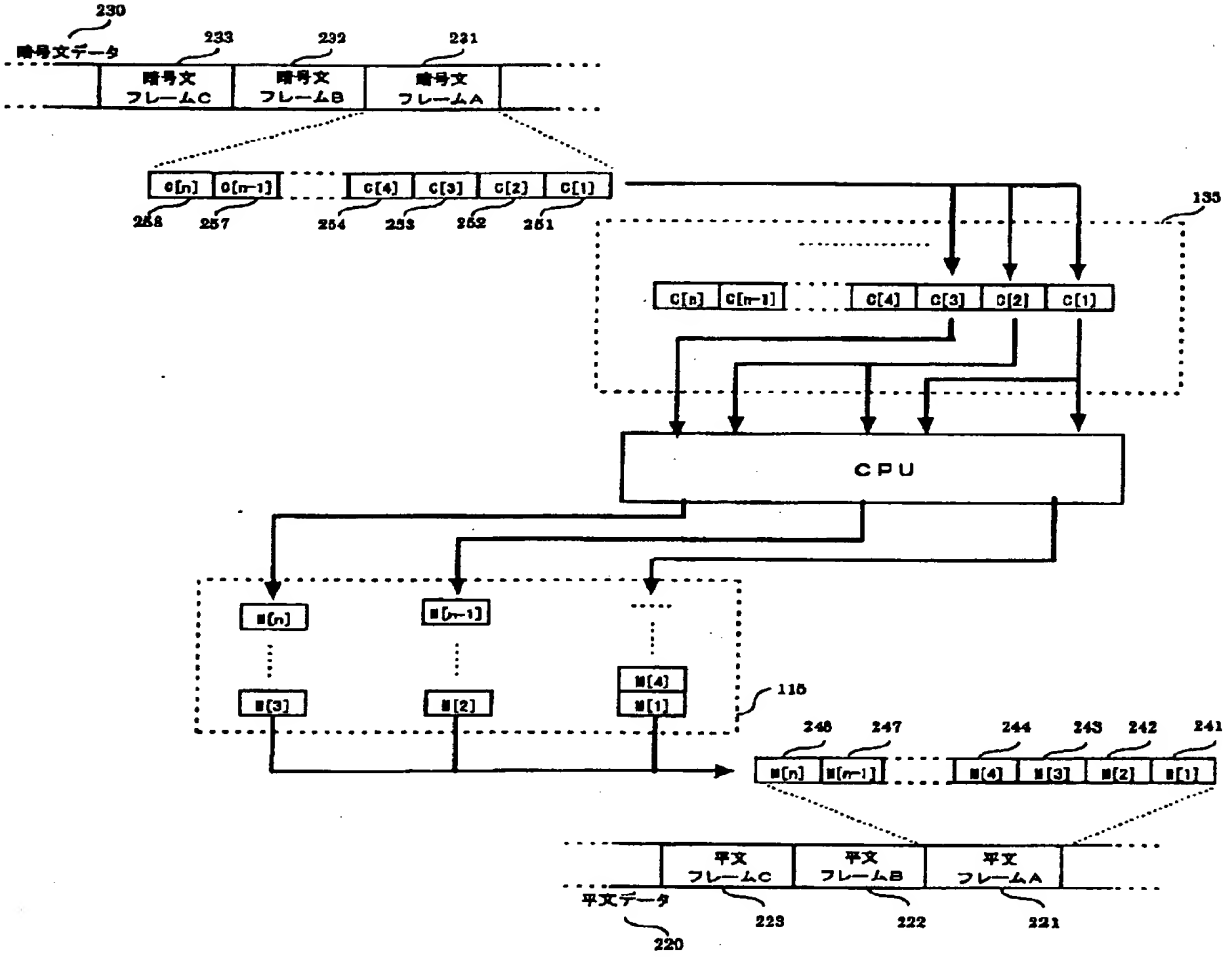
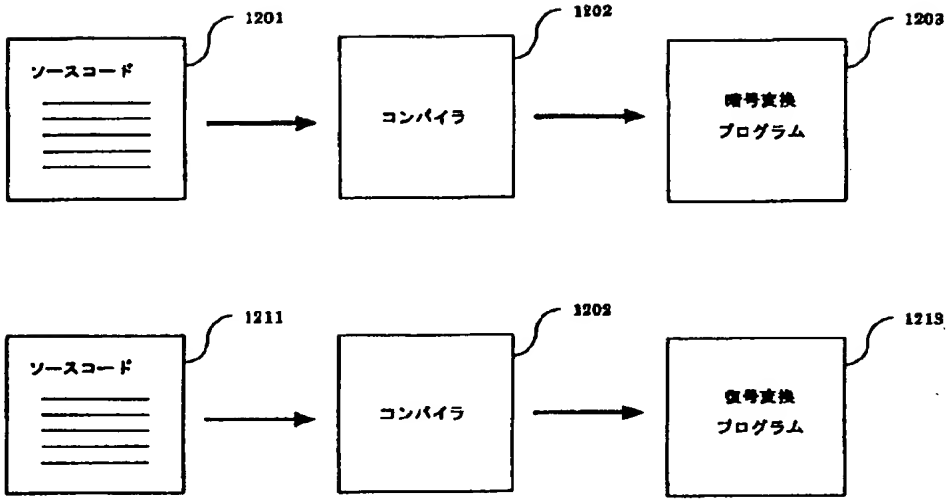

230
暗号文データ
233
232
231
暗号文 フレームC
暗号文 フレームB
暗号文 フレームA
C[n]
C[n-1]
C[4]
C[3]
C[2]
C[1]
258
257
254
253
252
251
135
CPU
M[n]
M[n-1]
M[4]
M[3]
M[2]
M[1]
115
248
247
244
243
242
241
平文 フレームC
平文 フレームB
平文 フレームA
平文データ
223
222
221
220

図 13

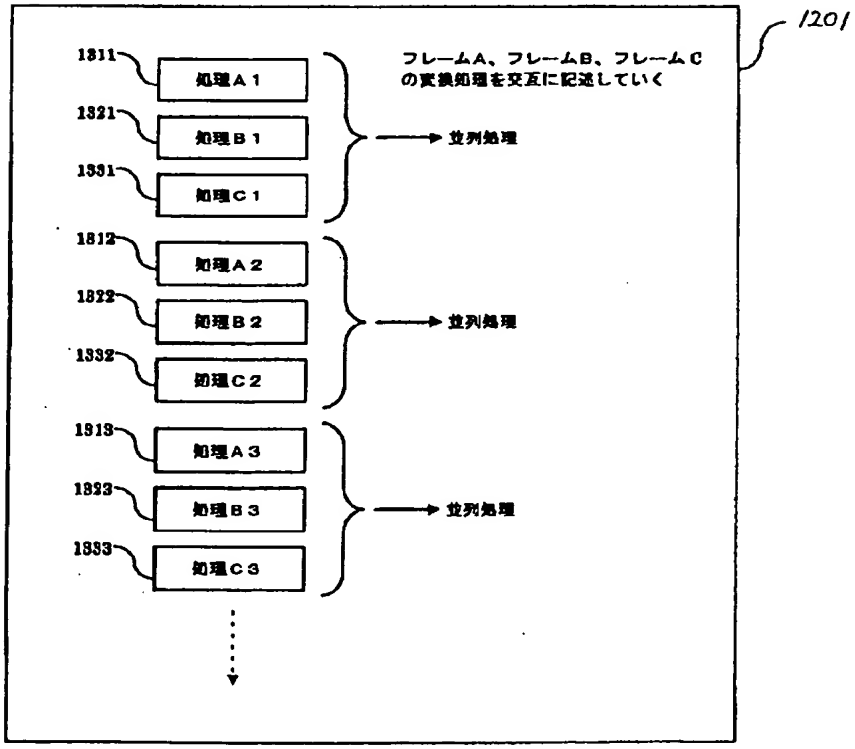
【図１４】

図　１４



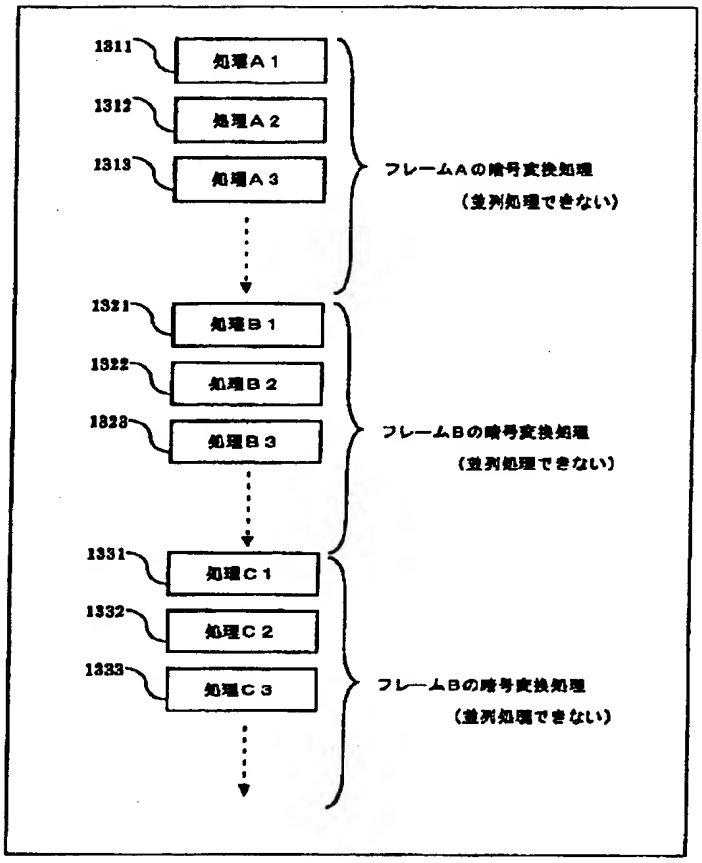
【図１６】

図　１６



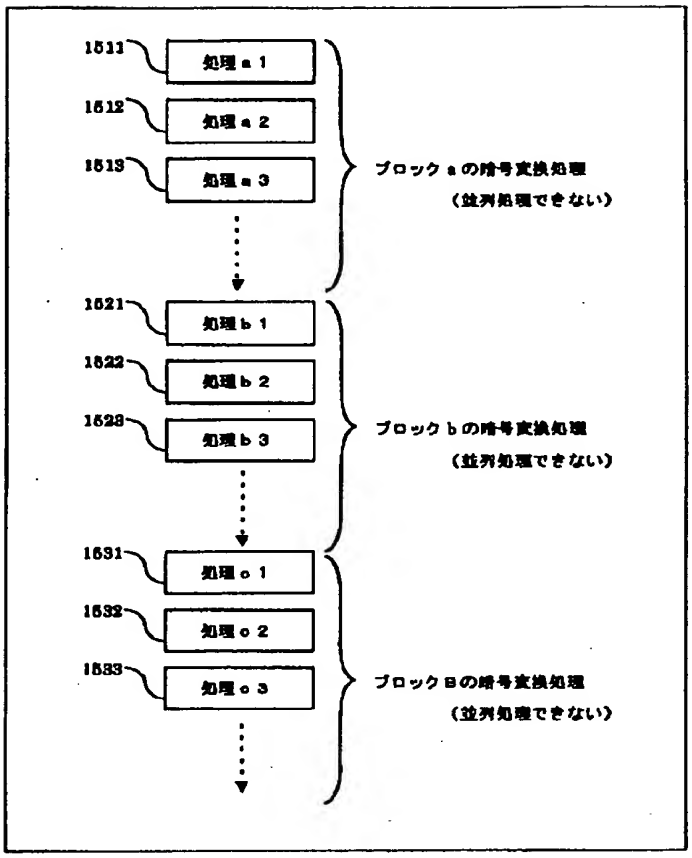
【図１５】

図　１５


1311
処理Ａ１
1312
処理Ａ２
1313
処理Ａ３
フレームＡの暗号変換処理
（並列処理できない）
1321
処理Ｂ１
1322
処理Ｂ２
1323
処理Ｂ３
フレームＢの暗号変換処理
（並列処理できない）
1331
処理Ｃ１
1332
処理Ｃ２
1333
処理Ｃ３
フレームＢの暗号変換処理
（並列処理できない）

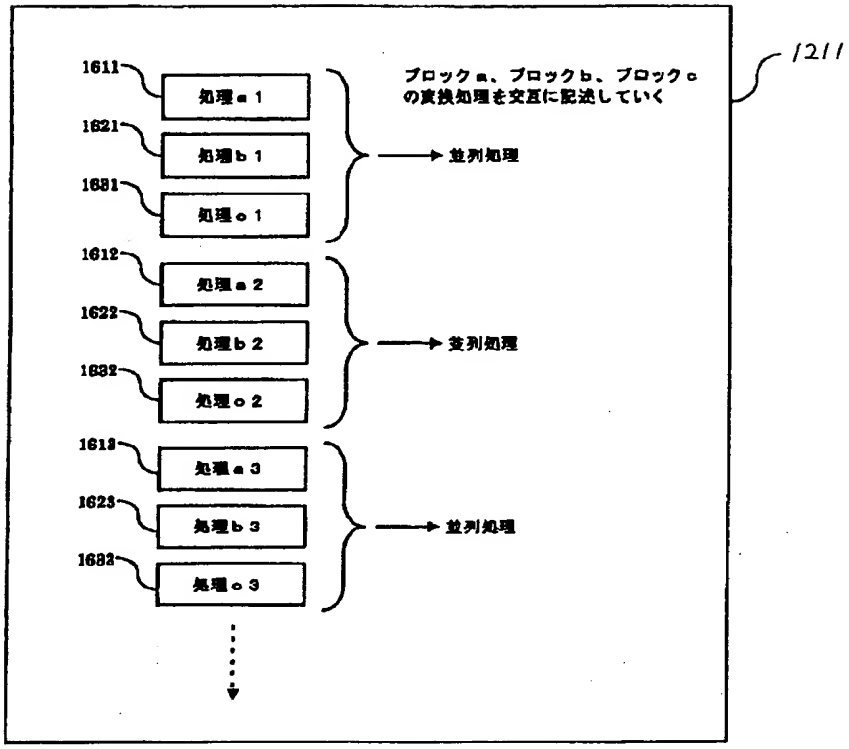
【図１７】

図　１７


1511
処理ａ１
1512
処理ａ２
1513
処理ａ３
ブロックａの暗号変換処理
（並列処理できない）
1521
処理ｂ１
1522
処理ｂ２
1523
処理ｂ３
ブロックｂの暗号変換処理
（並列処理できない）
1531
処理ｃ１
1532
処理ｃ２
1533
処理ｃ３
ブロックｃの暗号変換処理
（並列処理できない）

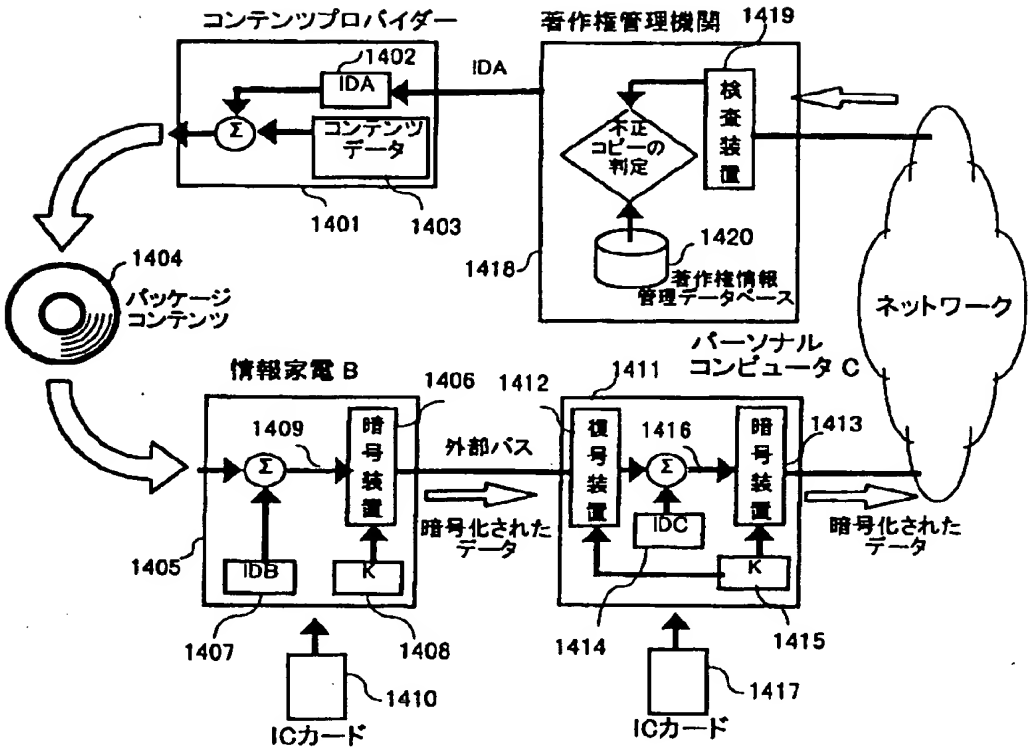
【図１８】

図　１８


1611
処理ａ１
1621
処理ｂ１
1631
処理ｃ１
並列処理
1612
処理ａ２
1622
処理ｂ２
1632
処理ｃ２
並列処理
1613
処理ａ３
1623
処理ｂ３
1633
処理ｃ３
並列処理
ブロックａ、ブロックｂ、ブロックｃ
の変換処理を交互に記述していく
211

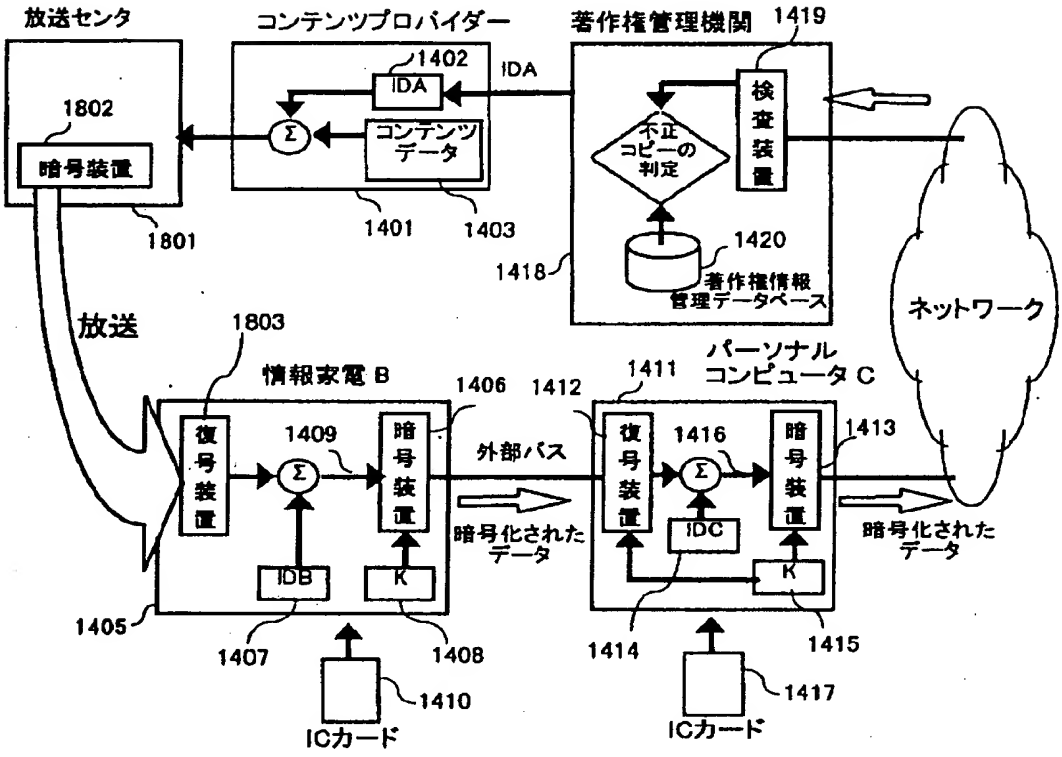
【図１９】

図　１９


コンテンツプロバイダー
著作権管理機関
1419
1402
IDA
IDA
検査装置
不正コピーの判定
コンテンツデータ
1401
1403
1420
1418
著作権情報管理データベース
1404
パッケージコンテンツ
ネットワーク
パーソナルコンピュータ C
情報家電 B
1406
1412
1411
1409
暗号装置
外部バス
復号装置
1416
暗号装置
1413
暗号化されたデータ
暗号化されたデータ
IDC
1405
IDB
K
K
1407
1408
1414
1415
1410
1417
ICカード
ICカード

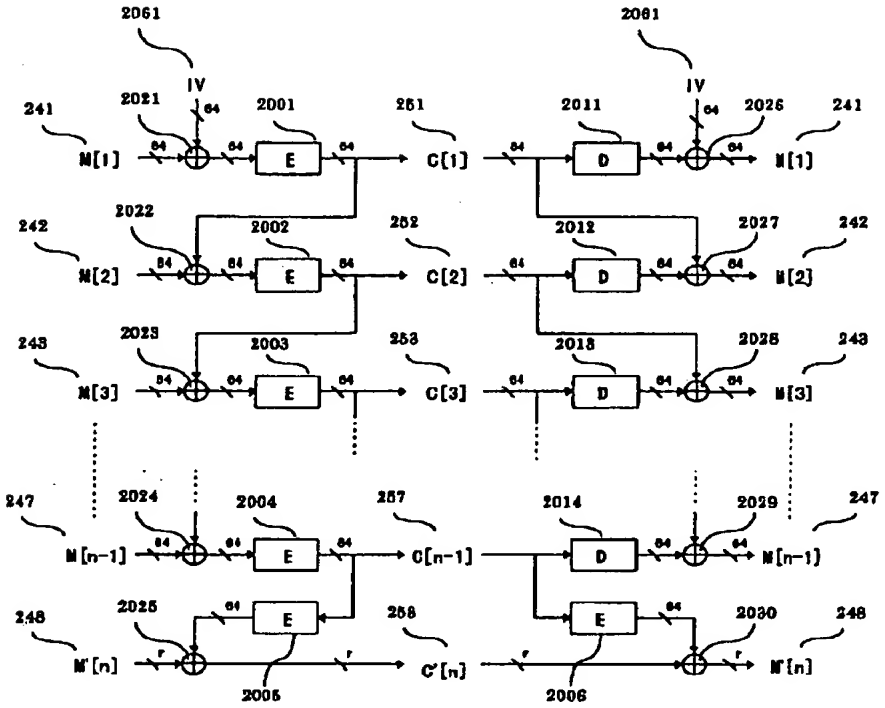
【図２３】

図 ２３


放送センタ
コンテンツプロバイダー
著作権管理機関
1419
1402
IDA
IDA
1802
暗号装置
Σ
コンテンツデータ
検査装置
不正コピーの判定
1420
著作権情報管理データベース
1418
1401
1403
1801
放送
1803
ネットワーク
情報家電 B
パーソナルコンピュータ C
1406
1412
1411
復号装置
1409
暗号装置
外部バス
復号装置
1416
暗号装置
1413
暗号化されたデータ
暗号化されたデータ
IDB
K
IDC
K
1405
1407
1408
1414
1415
1410
1417
ICカード
ICカード

【図２４】

図　２４



フロントページの続き

(72)発明者　古屋　聡一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　平畠　茂
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マルチメディアシステム開発本部内